



Instituto Universitário de Lisboa
Lisbon University Institute

Formulário

**Inteligência em Gestão
de Redes e Serviços**



Instituto Universitário de Lisboa
Lisbon University Institute

Rede Inteligente

Redes Inteligentes (IN): motivação

- Factores que levaram ao aparecimento da IN:
 - Economia / sociedade
 - Leis anti-monopólio nos EUA (desmembramento da AT&T).
 - Aumentar os *serviços* oferecidos pela rede telefónica
 - O custo para o utilizador não é o único factor competitivo
 - Alguns serviços que demonstraram ter grande sucesso:
 - » Número Verde e Número Azul
 - Introduzir rapidamente e com custos reduzidos novos *serviços* de telecomunicações num ambiente multi-vendedor
- Tecnologia:
 - A introdução da comutação digital
 - A utilização de uma sinalização digital (e.g., SS7) e separada dos circuitos de transporte dos dados do serviço (e.g., voz)
 - Capacidade dos sistemas computacionais
 - Utilização de conceitos/técnicas da Engenharia de Software (e.g., orientação a objectos, reutilização de software)

Redes Inteligentes (IN): motivação

Ecos da conf. “Mobile WiMAX, ISCTE 2008”

- *“We have to look from top to bottom.
Look for the cheap killer applications”*

Hamid Hagwami

- *“Take care of the cost of your services
(not the infrastructure)”*

Udo Duelberg

Redes Inteligentes: motivação

- Problemas na introdução de novos serviços (*pré-IN*):
 - Os serviços são fornecidos ao nível dos comutadores.
 - Distribuição dos serviços por **todos** os comutadores.
 - Os comutadores são de difícil programação e os seus programas complexos
 - Os comutadores são de diferentes fabricantes (intervenção dos fabricantes)
 - Certos serviços implicam que o comutador processe informação não-local mas comum a todos os comutadores
 - Ex: tradução de um número verde
 - Nestas condições demora muito tempo a desenvolver um novo serviço (usualmente 2 a 4 anos)

Redes Inteligentes: objectivos e princípios

• Objectivos:

- A introdução de novas possibilidades na rede de telecomunicações para facilitar e acelerar de uma forma eficaz e económica a implementação e a provisão de serviços num ambiente multi-vendedor
- A reutilização de “partes” de serviços
- A independência dos operadores dos fabricantes
- A interoperabilidade entre equipamentos de diferentes fabricantes e entre operadores
- Um melhor controlo e maior rapidez na introdução dos serviços e do seu funcionamento;
- Uma melhor adequação entre a oferta de serviços por parte do operador e a procura por parte dos utilizadores

Redes Inteligentes: objectivos e princípios

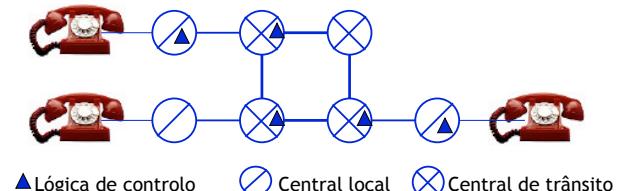
- Princípio da independência entre os recursos da rede e os serviços.
 - Os recursos são compostos por todas as funções que permitem tratar a **chamada básica** e funções ligadas à existência de equipamentos especiais tais como servidores de anúncios vocais ou pontos de conferência.
 - Os serviços são constituídos pelos algoritmos - **lógica de serviço** (software) - controlam os recursos e pelos dados utilizados no serviço.
 - A lógica de serviço pode ser alterada sem pôr em causa a rede.
 - O princípio da separação é concretizado pela definição de dois tipos de interfaces:



- A interface de programação (A), utilizada para a descrição da lógica e dos dados dos novos serviços. Permite que a rede seja uma plataforma independente dos serviços.
- A interface de comando dos recursos (B), interface normalizada que permite controlar os recursos físicos de diferentes fabricantes. Favorece a reutilização

Redes Inteligentes: objectivos e princípios

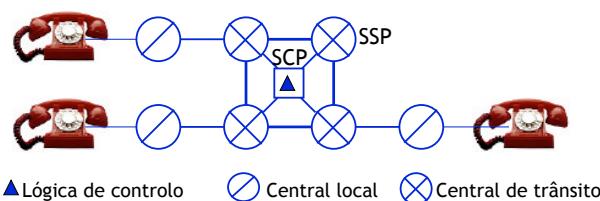
- Localização da lógica de serviço:
 - Antes da IN: A lógica do serviço é co-localizada com a comutação
 - A lógica do serviço está implantada ao longo do caminho de comutação



▲ Lógica de controlo ○ Central local ○ X Central de trânsito

Redes Inteligentes: objectivos e princípios

- Localização da lógica de serviço:
 - Fase 1 da IN: separação da “inteligência” da comutação

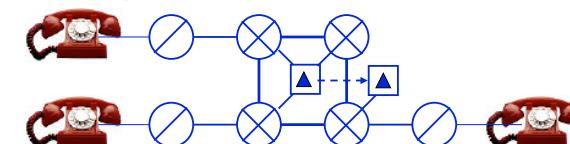


▲ Lógica de controlo ○ Central local ○ X Central de trânsito
SSP: Service Switching Point SCP: Service Control Point

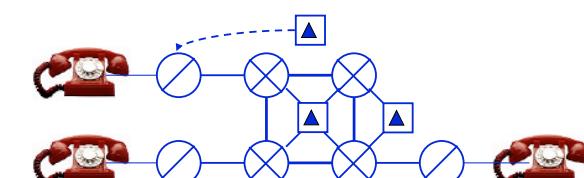
- Aspecto importante: disparo (*trigger*) dos serviços
 - Transferência do controlo da chamada para a lógica do serviço

Redes Inteligentes: objectivos e princípios

- Localização da lógica de serviço:
 - Fase 2 da IN: alocação flexível da “inteligência”

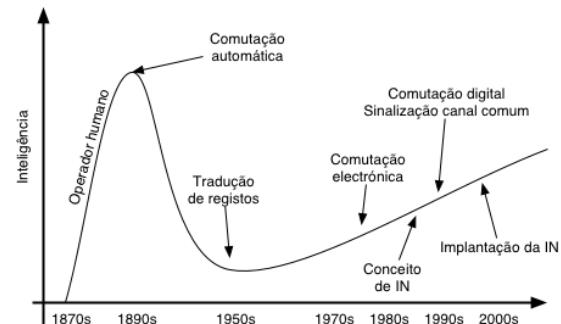


- Fase 3 da IN: “inteligência” a pedido



Redes Inteligentes: definição

- Não é o mesmo que inteligência artificial



Adaptado de "Intelligent Networks, Principles and applications"

Redes Inteligentes: definição

• Definição de Rede Inteligente

- A recomendação ITU-T Q1290 define a IN como: "um conceito arquitectural para a criação e fornecimento de serviços de telecomunicações" ..

Este conjunto arquitectural permite a introdução de novos serviços com grande flexibilidade e com novas possibilidades.

• Exemplos de serviços:

- Número verde, número azul
- Cartões pré-pagos
- Controlo de acessos (bloqueio de saída/entrada de chamadas)

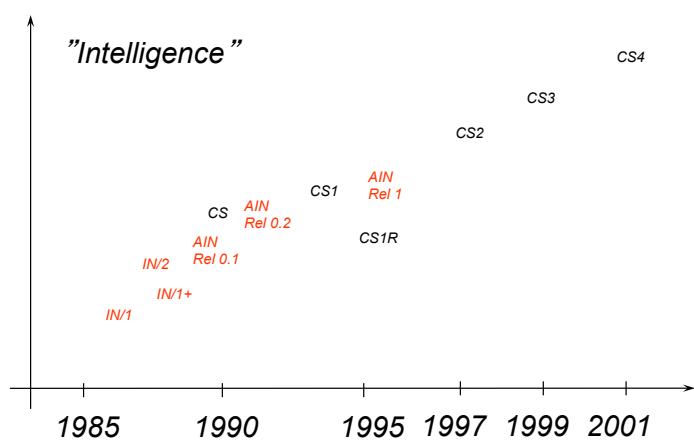
- A IN designa uma nova estruturação dos elementos da rede e não uma nova rede.
- No modelo conceptual são considerados simultaneamente a arquitectura de *hardware* e o enquadramento conceptual (*framework*) de *software*
- As arquitecturas definidas podem ser aplicadas à:
 - Rede telefónica comutada (POTS)
 - Rede de dados (e.g., Internet)
 - Redes móveis
 - Redes com integração de serviços (RDIS)

Redes Inteligentes: Modelo conceptual e arquitecturas (ITU-T)

- Definição do Modelo Conceptual (*IN Conceptual Model*):
 - O modelo conceptual é descrito na recomendação ITU-T Q1201 "Princípios da arquitectura da rede inteligente".
 - Não é uma arquitectura:
 - É uma metodologia para conceber e descrever arquitecturas para a IN
 - As diferentes "versões" do modelo conceptual IN ITU-T são descritas através de diferentes *Capability Sets (CS)*

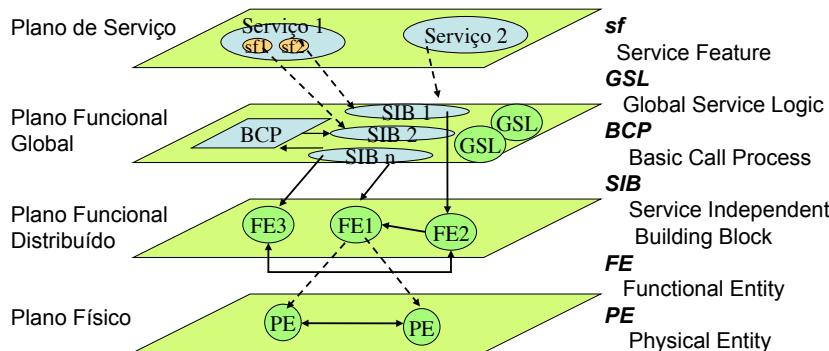
Recomendações Gerais	Recomendações para CS-x
Q.1200: IN Recommendations Structure	Q.12x0: Structure of IN CS-x
Q.1201: Principles of the IN Architecture	Q.12x1: Introduction to IN CS-x
Q.1202: IN Service Plane Architecture	Q.12x2: IN Service Plane Architecture for CS-x
Q.1203: IN Global Functional Plane Arch.	Q.12x3: IN Global Functional Plane Arch. for CS-x
Q.1204: IN Distributed Functional Plane Arch.	Q.12x4: IN Distributed Functional Plane Arch. for CS-x
Q.1205: IN Physical Plane Architecture	Q.12x5: IN Physical Plane Architecture for CS-x
Q.1208: General Aspects of the IN App Protocol	Q.12x8: IN Interface Recommendations for CS-x
Q.1290: Glossary of terms used in the definition of IN	Q.12x9: IN User Guide for CS-x

Evolução das normas para a Rede Inteligente



Planos do Modelo Conceptual da Rede Inteligente

- Composto por quatro planos (*planes*) com diferentes graus de abstração
- Um plano não é o mesmo que um nível (e.g., do modelo OSI)
 - Não existe o conceito de prestação de serviço de um plano ao plano superior, logo, não existem interfaces entre os diferentes planos (e.g., *duas formas de descrever o serviço de telefonia simples*)



Capability Set-1 (CS-1): Plano de serviços

Serviços de referência (atenção: são metas, não normalizados):

- Automatic Alternative Billing (AAB)
 - Abbreviated Dialing (ABD)
 - Account Card Calling (ACC)
 - Credit Card Calling (CCC)
 - Call Distribution (CD)
 - Call Forwarding (CF)
 - Completion of Call to Busy Subscriber (CCBS)
 - Conference Calling (CON)
 - Call Rerouting Distribution (CRD)
 - Destination Call Routing (DCR)
 - Follow-Me-Diversion (FMD)
 - Freephone (FPH)
 - Mass Calling (MAS)
 - Malicious Call Identification (MCI)
 - Premium Rate (PRM)
 - Security Screening (SEC)
- Def.: Um serviço é uma oferta comercial**
- Selective Call Forward on Busy/Don't Answer (SCF)
 - Split Charging (SPL)
 - Televoting (VOT)
 - Terminating Call Screening (TCS)
 - User-Defined Routing (UDR)
 - Universal Access Number (UAN)
 - Universal Personal Telecommunications (UPT)
 - Virtual Private Network (VPN)

Fonte [ITU Q1211]

Planos do Modelo Conceptual da Rede Inteligente

• Plano de serviços (*Service Plane*)

- Descrição dos serviços tal como “vistos” pelos utilizadores
 - Um serviço é uma oferta comercialposta à disposição por um fornecedor de serviço para os utilizadores satisfazerem uma necessidade de telecomunicações
- Descrição dos serviços em termos de elementos dos serviços (*service features*)
 - Um elemento de serviço é um componente de serviço que pode ser reutilizado por outros serviços
 - Não há qualquer referência à forma como os serviços são implementados
- Aspecto importante nos casos complexos: interacção de elementos (*feature interaction*)
 - Exemplos: *originating call screening* e *call forwarding*
- Exemplo de serviços: Número verde e Quiosque telefónico (*Helpdesk*)

Capability Set-1 (CS-1): Plano de serviços

Elementos de serviço (*service features*): lista não completa

- Abbreviated Dialing (ABD)
- Attendant (ATT)
- Authentication (AUTC)
- Authorization Code (AUTZ)
- Call Distribution (CD)
- Call Forwarding (CF)
- Call Forwarding on BY/DA (CFC)
- Call queuing (QUE)
- Call transfer (TRA)
- Call waiting (CW)
- Closed user group (CUG)
- Consultation calling (COC)
- Customer profile management (CPM)
- Customised recorded announcement (CRA)
- Customised ringing (CRG)
- One number (ONE)
- Origin dependent routing (ODR)
- Originating call screening (OCS)
- Originating user prompter (OUP)
- Personal numbering (PN)
- Reverse Charging (REVC)
- Split Charging (SPLC)
- Terminating call screening (TCS)
- Time dependent routing (TDR)

Def. 1: Um elemento de serviço representa um aspecto particular de um serviço

Def. 2: Um serviço é descrito por um ou mais elementos de serviço obrigatórios (*core*) e zero ou mais elementos de serviço opcionais.

Fonte [ITU Q1211]

Capability Set-1 (CS-1): Plano de serviços

- Tabela: Serviços vs. Elementos de serviço (não completa)

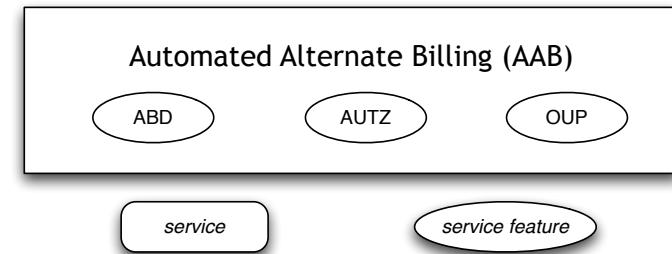
	ABD	AUTZ	ONE	OCS	REVC	SPLC
ABD	Core					
ACC	Core	Core				
CCC	Opt.	Core				
FPH			Core		Core	
OCS				Core		
SPL						Core

Capability Set-1 (CS-1): Plano de serviços

- Exemplo: Serviço de Automated Alternate Billing (AAB)

O serviço AAB permite a um utilizador utilizar qualquer terminal e debitar a chamada numa outra conta (tipicamente a sua).

- Número abreviado de acesso ao serviço (ex. 707351)
- Número de identificação do utilizador e palavra de passe
- Número a contactar



Planos do Modelo Conceptual da Rede Inteligente

• Plano funcional global (*Global Functional Plane*)

- Plano onde os operadores descrevem os serviços:
 - Através da definição da lógica global do serviço (*Global Service Logic*)
- A rede é modelizada como uma “máquina virtual” única e global
- Na *GSL* os serviços são descritos recorrendo a:
 - SIBs: Service Independent Building Blocks**
 - Os SIBs são componentes de serviço independentes dos serviços, dos elementos de serviço, e da sua implementação
 - Componentes que os fornecedores de serviços devem implantar na sua rede. Um elemento de serviços é implementado por uma ou mais SIBs
 - BCP: Basic Call Process** (SIB especial): Tratamento da chamada básica. A partir da qual os serviços são desencadeados



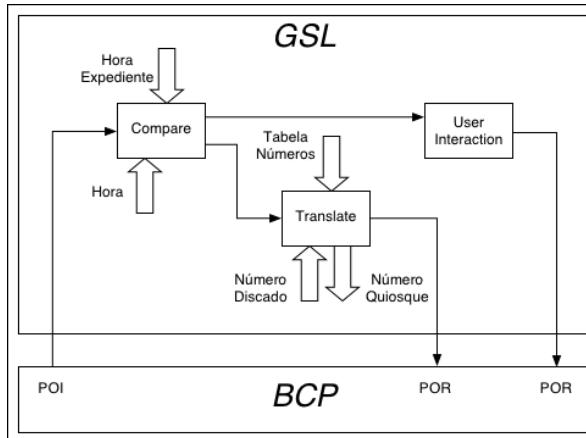
Planos do Modelo Conceptual da Rede Inteligente

• Plano funcional global (*Global Functional Plane*)

- Um serviço neste plano corresponde a um encadear de SIBs. Descreto através de um *service script*:
 - que começa num ponto preciso do tratamento da chamada: “*Point of Initiation*” (POI), onde é transferido o controlo entre o processamento de chamada básico (BCP) e o serviço,
 - quando toda a cadeia de SIB’s for executada o controlo é devolvido ao processamento de chamada básica num “*Point of Return*” (POR).
- Uma cadeia de SIB’s para um dado serviço, o seu POI e POR(s), constituem a sua lógica global de serviço (GSL)

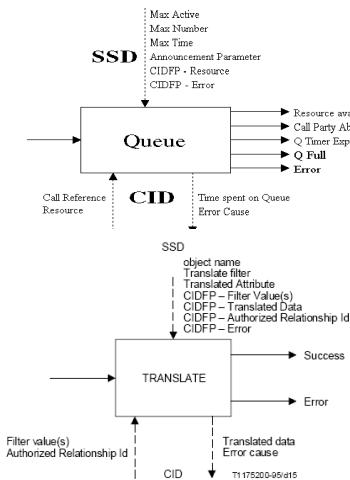
Planos do Modelo Conceptual da Rede Inteligente

- Plano funcional global: Exemplo “Quiosque telefónico”



CS-1: Plano Funcional Global

- Representação dos (SIB) no CS-1



- SIB descrita por:

- Pontos lógicos de entrada/saída
 - Um ponto lógico de entrada
 - Um ou mais pontos de saída
- Dados:
 - Referentes ao serviço: SSD
 - Max Active, Translate Filter
 - Referentes à chamada: CID
 - Call Reference, Filter value(s)

- SIB suporta:

- Controlo de fluxo (vários pontos lógicos de saída:
 - Resource Available, Q Full, Error)
- Alteração dos dados CID
 - Translated Data

(Figuras retiradas de [ITU95a])

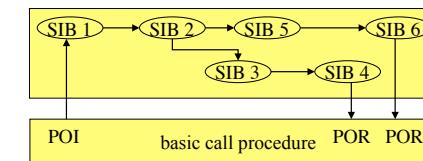
CS-1: Plano Funcional Global

- Service Independent Building Blocks (SIB) do CS-1

- *Algorithm*: efectua uma operação aritmética (+,-).
- *Charge*: permite aplicar uma tarifa especial.
- *Compare*: efectua uma comparação entre dois parâmetros, um do tipo SSD e o outro CID.
- *Distribution*: permite a um utilizador repartir as suas chamadas por diferentes saídas lógicas.
- *Limit*: Limita o número de chamadas de rede inteligente filtrando-as com base em certos critérios de acordo com os parâmetros especificados pelo fornecedor do serviço
- *Log Call Information*: regista certas informações relativas a uma chamada num ficheiro.
- *Queue*: permite colocar chamadas em espera.
- *Screen*: permite verificar se um parâmetro dinâmico pertence ou não a uma lista de indicadores estática.
- *Service Data Management*: permite manipular dados relativos a um utilizador.
- *Status Notification*: permite conhecer o estado dos recursos da rede (ex: estado da linha)
- *Translate*: traduz um parâmetro de entrada num parâmetro de saída utilizando como tabela um ficheiro cuja identificação é um parâmetro estático.
- *User Interaction*: permite a troca de informação entre o utilizador e a rede. (ex: anúncio vocal)
- *Verify*: verifica que uma informação recebida está sintaticamente correcta.

CS-1: Plano Funcional Global

- POI e POR na BCP definidos pelo CS-1



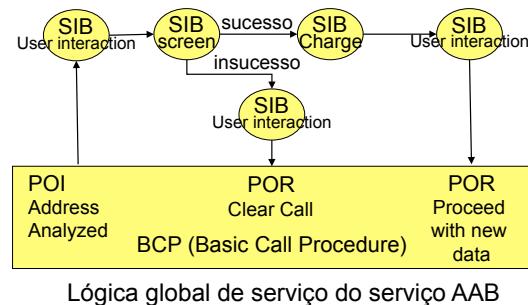
Pontos de início (POI)	Pontos de retorno (POR)
Call originated Address Collected Address Analyzed Prepared to Complete Call Call Acceptance No Answer Busy Active State End of Call	Continue with existing data Proceed with new data Clear Call Handle as Transit Enable call party handling Initiate Call

CS-1: Plano Funcional Global

- Exemplo: Serviço de **Automated Alternate Billing (AAB)**

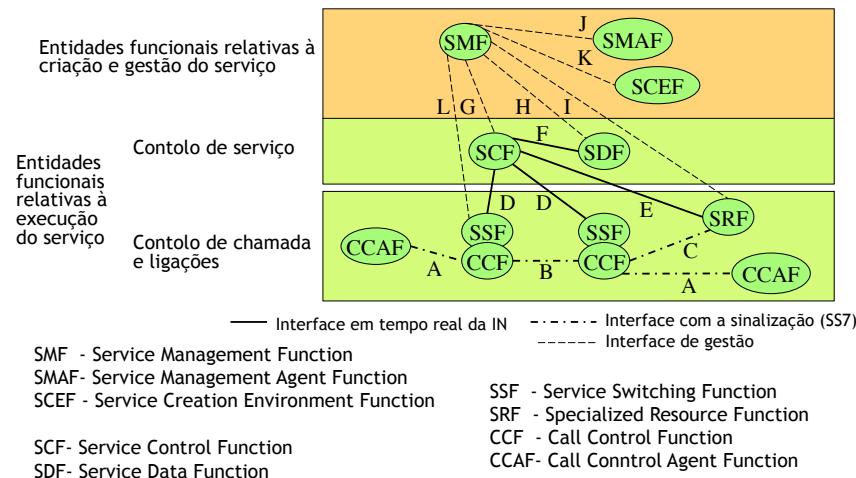
O serviço AAB permite a um utilizador utilizar qualquer terminal e debitar a chamada numa outra conta.

- Número de acesso ao serviço
- Número de identificação do utilizador e palavra de passe
- Número a contactar



Planos do Modelo Conceptual da Rede Inteligente

- Arquitectura do plano funcional repartido



Planos do Modelo Conceptual da Rede Inteligente

- **Plano funcional repartido (Distributed Functional Plane)**

- DFP: Visão distribuída dos serviços na rede
 - Visão mais “correcta” que a visão monolítica do GFP tendo em conta a distribuição de funcionalidade na rede
 - Ex: interacção entre centrais de comutação
 - Descrição da arquitectura funcional da rede inteligente em termos das entidades funcionais distribuídas na(s) rede(s) que a implementa
- No DFP são identificadas:
 - *Functional entities (FE)*: distribuídas na rede:
 - Uma entidade funcional representa um grupo de funções localizadas num só ponto e constitui um subconjunto do conjunto das funções necessárias para fornecer um serviço.
 - Executam acções (*Functional Entity Actions: FEA*)
 - A execução de uma SIB pode envolver uma ou mais entidades funcionais
 - Entidades funcionais de
 - » Criação e gestão do serviço
 - » Execução do serviço (controlo de chamada e controlo de serviço)
 - Os pontos de detecção (*Detection Points*): implementações dos POIs
 - Os fluxos de informação entre FEs (representados formalmente com SDL e MSC)

Planos do Modelo Conceptual da Rede Inteligente

Entidades Funcionais do Plano Funcional Repartido (DFP)

Gestão e criação do serviço

- **SMF-Service Management Function**: controlo e gestão da implantação, provisão e operação do serviço
- **SMAF-Service Management Agent Function**: fornece a interface entre os gestores de serviço e o SMF
- **SCEF-Service Creation Environment Function**: permite aos serviços serem definidos, desenvolvidos, testados e incluídos na SMF: o resultado é a lógica de serviço e os dados do serviço

Controlo do serviço

- **SCF-Service Control Function**: contém a lógica do serviço da IN e efectua o processamento necessário ao serviço. Controla as funções de controlo de chamada resultantes dos pedidos do serviço
- **SDF-Service Data Function**: Gere os acessos aos dados do serviço e da rede. Fornece ao SCF uma visão lógica dos dados escondendo a sua implementação

Planos do Modelo Conceptual da Rede Inteligente

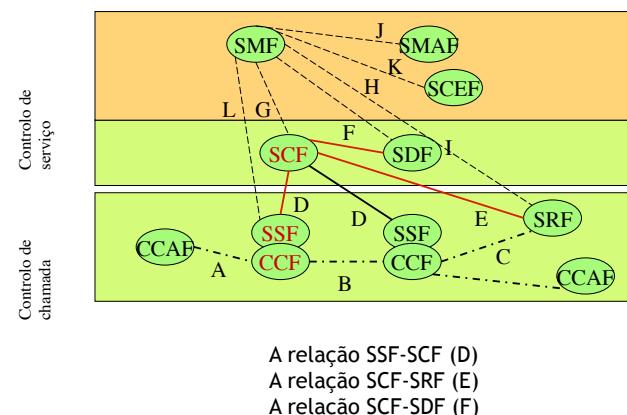
Entidades Funcionais do Plano Funcional Repartido (DFP)

Controlo da chamada e ligações

- *CCAF-Call Control Agent Function* representa o acesso dum utilizador à rede
- *CCF-Call Control Function*: trata e controla a chamada e a ligação. Não tem qualquer implementação dos serviços, mas reconhece pedidos de serviços podendo delegar o controlo da chamada
- *SSF-Service Switching Function*: constitui a interface entre o CCF e a SCF; permite trocas de informação entre CCF e SCF; e que a SCF controle a CCF
- *SRF-Specialized Resource Function*: permite o acesso a outras entidades da rede especializadas (ex. servidores de avisos áudio)

CS-1: Plano Funcional Repartido

- Relações entre entidades funcionais descritas no CS-1



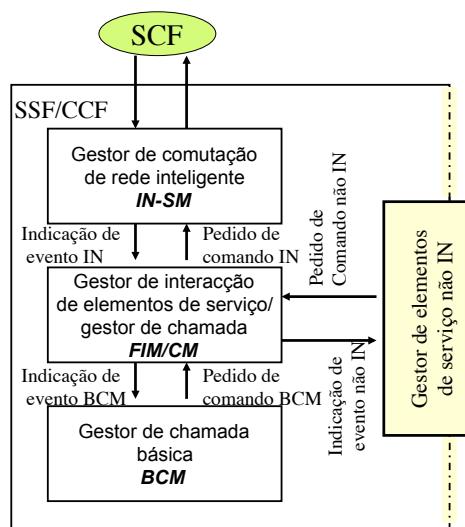
Planos do Modelo Conceptual da Rede Inteligente

Entidades Funcionais (cont.)

- *Information flows*
 - Como diversas entidades funcionais estão envolvidas na realização de um serviço, elas tem que trocar fluxo de informação (*Information Flow - IF*): (A,B,C), (D,E,F), (G,H,I,J,K,L)
- **Relação com o plano funcional global:**
 - A interface de programação pode situar-se nas entidades SDF, SMF ou SMAF
 - A interface de comando dos recursos situa-se entre as entidades SCF e SDF (base de dados) e as entidades SSF, CCF, CCAF e SRF (elementos da rede).
 - As entidades SCF e SDF representam a “inteligência” da rede isto é a lógica e os dados do serviço.
As outras entidades representam os recursos da rede.

CS-1: Plano Funcional Repartido

- Relação SSF/CCF



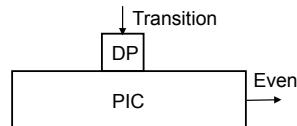
- O **BCM** é a entidade do CCF que gera as chamadas e controla as ligações. Coloca em prática o tratamento de chamada. É encarregue de detectar os eventos que podem conduzir à evocação das instâncias da lógica de serviço através dos pontos de detecção

- O **IN-SM** é a entidade do SSF que interage com o SCF para fornecer serviços. Fornece ao SCF uma visão abstrata das actividades do tratamento de chamada ou ligações e das capacidades e recursos do SSF/CCF. Detecta os eventos do tratamento de chamada e conexões que devem ser reportados às instâncias da lógica de serviço.

- O **FIM/CM** é a entidade do SSF que fornece os mecanismos que permitem ter diversas instâncias concorrentes da lógica de serviço da IN e não-IN na mesma chamada

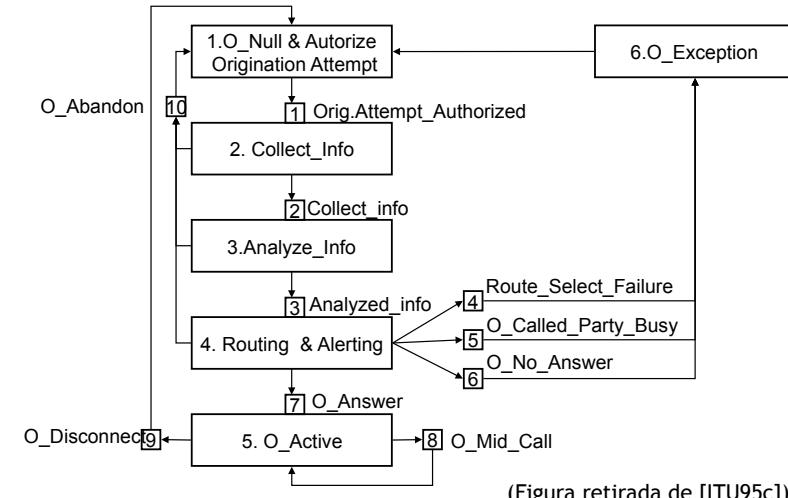
CS-1: Plano Funcional Repartido

- O modelo de tratamento de chamada no DFP
- O BCM fornece um modelo de tratamento de chamada que consiste numa descrição de alto nível das actividades do CCF por uma máquina de estados finitos (*Basic Call State Model - BSCM*)
 - Identificando o chamador (Originating) e chamado (Terminating)
- Identifica os pontos do tratamento da chamada onde a lógica de serviço está autorizada a interagir, nomeadamente:
 - *Point in Calls (PIC)*, que identificam as actividades da CCF necessárias a um estado do tratamento de chamada.
 - *Detection Points (DP)*, pontos de detecção que indicam os pontos do tratamento da chamada ou da ligação onde pode ocorrer uma transferência de controlo (Representam a implementação no DFP dos POIs do GFP)
 - *Transition*, que indicam o fluxo normal do tratamento da chamada/ligação entre dois PIC.
 - *Events*, as causas das transições.



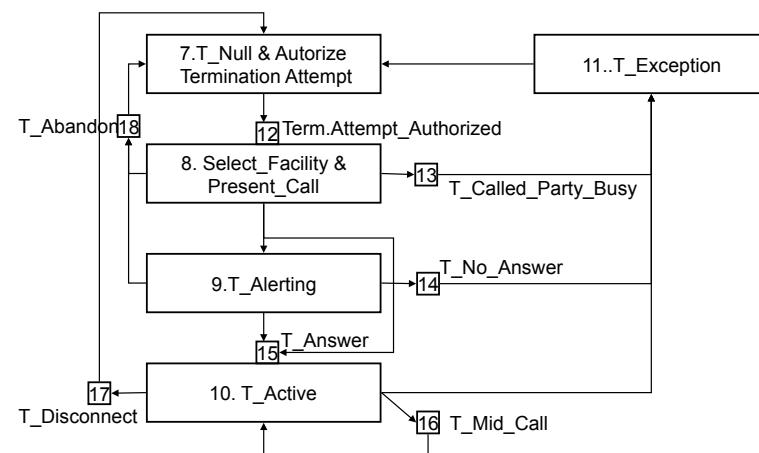
CS-1: Plano Funcional Repartido

- O O-Basic Call State Model (O-BSCM)



CS-1: Plano Funcional Repartido

- O T-Basic Call State Model (T-BSCM)



CS-1: Plano Funcional Repartido

- Descrição de Detection Points (DP)
- Os DP são caracterizados por atributos:

- O mecanismo de armar, i.e., o modo como o DP é armado. Um DP tem que ser previamente armado para poder avisar o SCF. Os DP podem ser armados estáticamente ou dinamicamente:
 - *Trigger Detection Point* - é armado estaticamente pelo SMF quando do provisionamento do serviço
 - *Event Detection Point* - é armado dinamicamente pelo SCF durante a execução dum serviço associado a uma chamada duma dada relação SSF-SCF, e mantém-se armado até ser detectado ou até ao final dessa relação.
- Os critérios, são condições que devem ser verificadas em conjunto com o armar dum DP estático para que o SCF seja avisado que um DP foi encontrado durante o tratamento de uma chamada. Exemplo: encontrar um nº específico 800

CS-1: Plano Funcional Repartido

- Os DP são caracterizados por atributos (cont.):

- A relação entre o SSF e o SCF** estabelece-se durante uma chamada quando o SSF avisa o SCF que um DP armado é encontrado e que os critérios associados são verificados. Diz-se que a relação é do tipo de *comando* se o SCF poder influenciar o desenrolar do tratamento da chamada, caso contrário diz-se que é do tipo *monitorização*.

- Suspensão:**

Se o SSF suspender o processamento de chamada para permitir que o SCF actue sobre esse processamento uma vez que este foi avisado do encontro de um DP armado e cujos critérios foram verificados. Neste caso o SSF informa o SCF do encontro do DP e da suspensão do processamento e aguarda instruções por parte do SCF, i.e. envia um *Request*. No caso de não suspensão, o SSF informa da mesma forma o SCF do facto de ter encontrado um DP mas não aguarda pela resposta, i.e., envia uma *Notification*.

CS-1: Plano Funcional Repartido

Tipo de DP	Armamento	Critérios	Relação de controlo da IN	Suspensão
TDP-R	Estático	Especifico do DP	Estabelece relação de comando	Sim
TDP-N	Estático	Especifico do DP	Estabelece e termina relação de monitorização	Não
EDP-R	Dinâmico	Nenhum	No contexto duma relação de comando existente	Sim
EDP-N	Dinâmico	Nenhum	No contexto duma relação de comando ou monitorização existente	Não

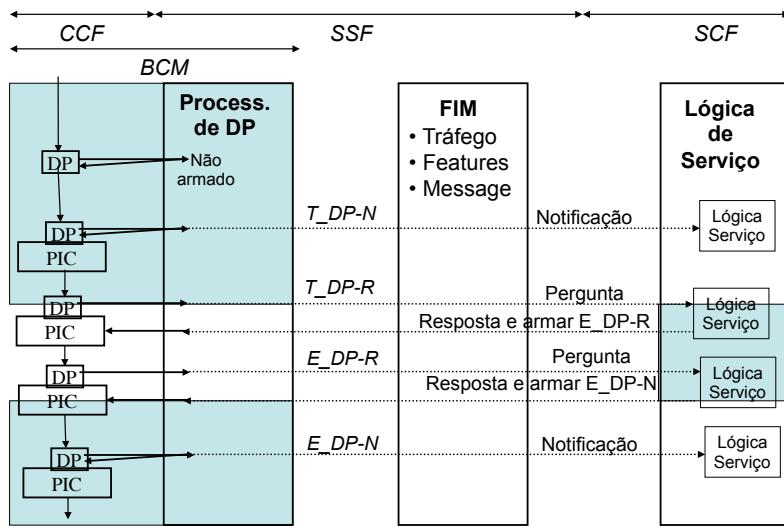
CS-1: Plano Funcional Repartido

- O gestor de comutação de rede inteligente IN-SM
 - O IN-SM é a entidade do SSF que interage com o SCF para fornecer serviços. Fornece ao SCF uma visão abstracta das actividades do tratamento de chamada ou ligações e das capacidades e recursos do SSF/CCF. Detecta os eventos do tratamento de chamada e conexões que devem ser reportados às instâncias da lógica de serviço.
 - Ao SCF é apresentado um modelo abstracto do funcionamento do processamento de chamada com base num modelo de estados de comutação de rede inteligente.
 - Neste modelo o SCF tem a visão de uma parte isolada da chamada: Call-Segment. Existirá um Call-Segment chamador e um chamado. Um tem associado o O-BSCM e outro o T-BSCM.
 - O Call-Segment faz referência aos recursos físicos e aos processos modelados pelo BSCM
 - O SCF não tem acesso directo ao Call-Segment mas sim a uma representação abstracta.
 - O SCF comanda as vias de comunicação e de conexão de acordo com os BSCMs.

CS-1: Plano Funcional Repartido

- Gestor de interacção de elementos de serviço/gestor de chamada FIM/CM
 - O FIM/CM é a entidade do SSF que fornece os mecanismos que permitem ter diversas instâncias concorrentes da lógica de serviço da IN e não IN na mesma chamada.
 - O CM tem por função gerir os diferentes elementos dos “Call-Segments”
 - O CM tem a missão de coordenar as notificações dos eventos entre os BSCMs, a suspensão e retoma do processamento de chamada entre os BSCMs.
 - O FIM fornece os mecanismos que asseguram a coordenação entre os diversos elementos de serviço (IN ou não) que podem estar activos simultaneamente, mecanismos de prioridade exclusão. Selecciona a instância da lógica de serviço que invoca um dado DP, bloqueando todas as outras. Pode recusar a entrada em operação simultânea de instância da lógica de serviço IN ou não-IN que comandam a chamada ou a ligação.
 - É complexo ...

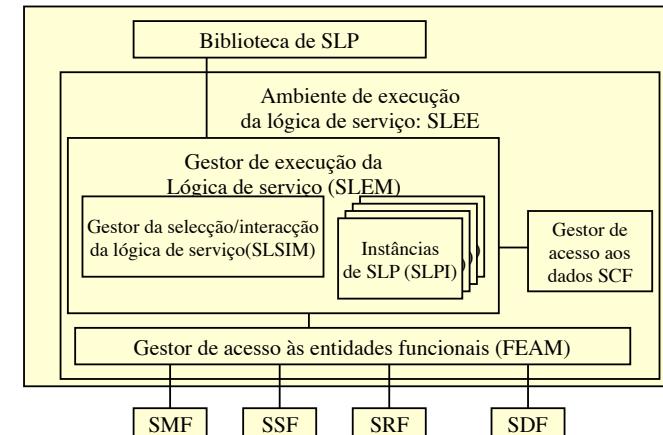
CS-1: Plano Funcional Repartido



CS-1: Plano Funcional Repartido

O modelo do SCF

- A função do SCF é executar a lógica de serviço que é fornecida como forma de um programa de processamento desta: Service Logic Processing program: SLP



CS-1: Plano Funcional Repartido

- O SCF é composto por:
 - Uma biblioteca de *SLP - Service Logic Processing*
 - Um ambiente de execução dos SLP: *SLEE - Service Logic Execution Environment*, constituído por:
 - Um gestor de execução da lógica de serviço: *SLEM-Service logic Execution Manager*, que gera e comanda todas as ações da execução da lógica de serviço e que contém:
 - Instâncias do SLP: *SLP Instance - SLPI*
 - Gestor de selecção/interacção da lógica de serviço (*SLSIM:Service Logic Selection/Interaction Manager*) responsável por seleccionar um SLP e de criar uma instância. Assegura também a gestão das interacções entre os diversos SLPs activos em simultâneo numa mesma chamada. A selecção de cada SLP depende do parâmetro *Service Key* nas mensagens *I_DP*.
 - Um gestor de acesso aos dados do SCF: *SCF Data Access Manager*, que permite o acesso à informação partilhadas e persistentes do SCF, isto é perduram para além da vida dum SLPI.
 - Um gestor de acesso às entidades funcionais: *FEAM- Functional Entity Access Manager*, que permite ao SCF trocar informações com todos as outras entidades funcionais gerindo diferentes protocolos. (SMF, SSF, SDF e SRF)

Relação entre o GFP e o DFP

- O plano funcional global contém as lógicas globais de serviço, GSL, cada uma composta por uma cadeia de SIBs incluindo o BCP com os pontos de início (POI) e retorno (POR).
- Cada SIB é realizado no plano funcional repartido por ações de entidades funcionais (*Functional Entity Action - FEA*).
- Cada FEA é numerada por *XYYZ* em que:
 - X* representa o n.º da entidade funcional,
 - YY* representa o n.º do SIB
 - Z* é um número distinto para cada FEA do mesmo SIB e da mesma FE.

FE	No X
CCF/SSF	2
SRF	3
SDF	4
SCF	9

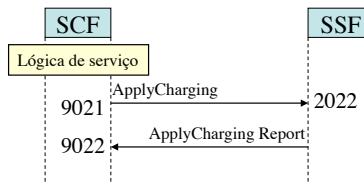
Nome do SIB	No YY
BCP	00
Algoritm	01
Charge	02
Compare	03
Distribution	04
Limit	05
Log Call Info.	06

Nome do SIB	No YY
Queue	07
Screen	08
Service Data Manag.	09
Status Notification	10
Translate	11
User Interaction	12
Verify	13

- Um SIB é representado no plano funcional repartido pela enumeração das FEAs que participam na sua realização quer façam parte da mesma FA ou não. É necessário indicar o sentido do fluxo de informação para ter a representação completa do SIB.

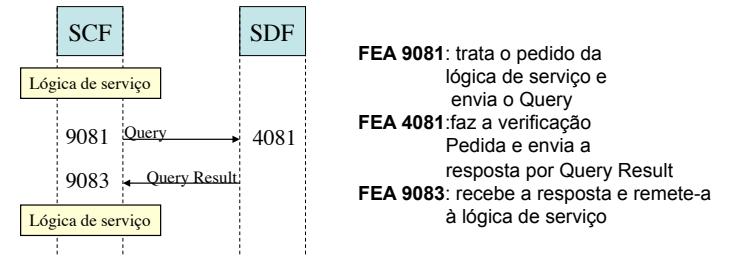
Relação entre o GFP e o DFP (Ex. 1 SIB Charge)

- O SIB charge permite aplicar uma tarifa particular às chamadas.
- É realizado pelas entidades SCF e SSF que interagem para tratar as informações de tarifação.
- O SCF pode pedir ao SSF para:
 - produzir um registo relativo à chamada em curso.
 - aplicar características particulares de tarifa à chamada em curso com envio ou não de um relatório (figura).
 - Monitorizar um evento reportando a taxação com relatório dessa ocorrência



Relação entre o GFP e o DFP (Ex. 2 SIB Screen)

- O SIB Screen permite determinar se um identificador pertence a uma lista, esta lista encontra-se guardada no SDF. Este SIB é realizado pela interacção do SCF e SDF.



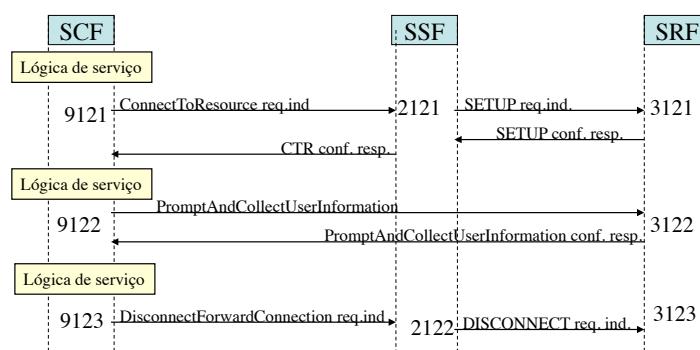
FEA 9081: trata o pedido da lógica de serviço e envia o Query

FEA 4081: faz a verificação Pedida e envia a resposta por Query Result

FEA 9083: recebe a resposta e remete-a à lógica de serviço

Relação entre o GFP e o DFP (Ex. 3, SIB UI)

- O SIB User Interaction (UI) permite a troca de informações entre um utilizador e a rede para responder às necessidades da lógica de serviço.
- Estas informações podem ser: Anúncios de voz, recolha de dados do utilizador.
- As entidades cooperantes na recolha de dados são: SCF, SSF e SRF



Relação entre o GFP e o DFP (POIs)

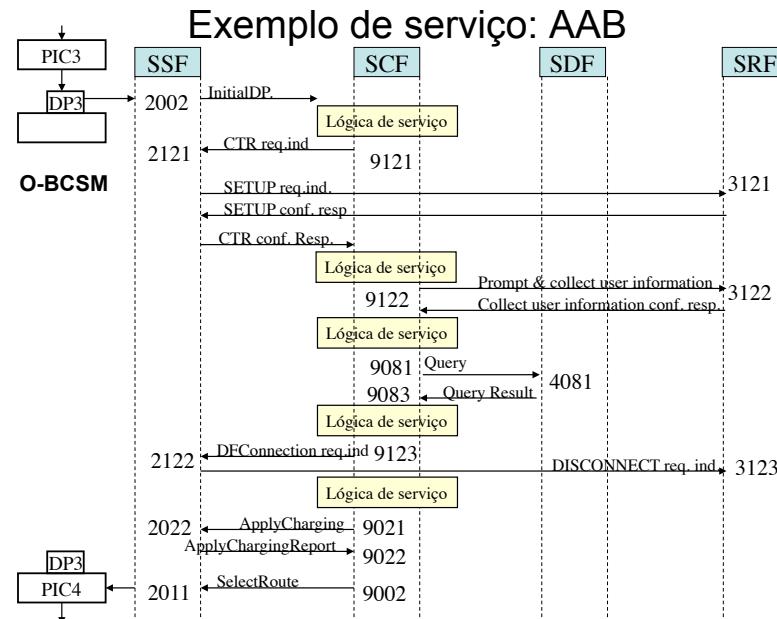
- Os POIs correspondem a etapas do processamento de chamada onde um serviço de IN pode ser evocado sendo o processamento de chamada suspenso.
- Os POIs vão corresponder no plano funcional repartido aos DP-R. Um POI pode corresponder a DP-R diferentes.

Point of Initiation (POI)	Detection Point (DP)
Call Originated	Origination_Attempt_Authorized
Address Collected	Collect_Information
Address Analyzed	Analyzed_Information
Prepared to complete call	T_Attempt_Authorized
Busy	Route_Select_Failure O / T_Called_party_Busy
No Answer	O / T_No_Answer
Call Acceptance	O / T_Answer
Active State	O / T_Mid_Call
End of Call	O / T_Abandon O / T_Disconnect

Relação entre o GFP e o DFP (PORs)

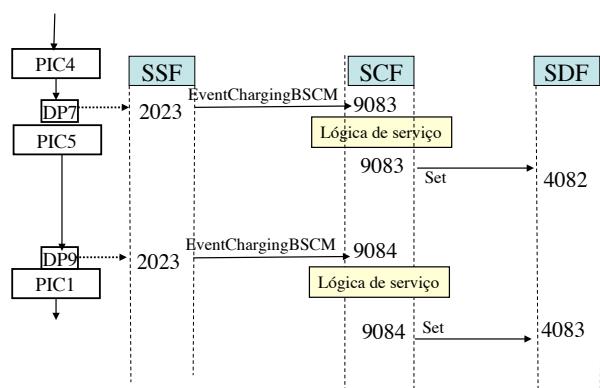
- Os PORs são pontos onde é retomado o processamento de chamada depois de executada a cadeia de SIBs.
- Os PORs do GFP podem ser representados por DP-R, ou PIC no DFP.

Point of Return (POR)	Detection Point (DP) ou Point in Call (PIC)
Continue with same data	Retorno ao DP-R no qual o serviço foi lançado
Proceed with new data	Retorno a um PIC específico do serviço
Handle as transit	PIC 3 ou PIC 5
Clear call	O_Null/T_Null
Enable call party handling	Retorno ao DP-R no qual o serviço foi lançado
Initiate call	PIC 3 ou PIC 5 dum novo BCSM



Exemplo de serviço: AAB (cont.)

O-BCSM (Não há qualquer E_DP-R logo modo monitor)

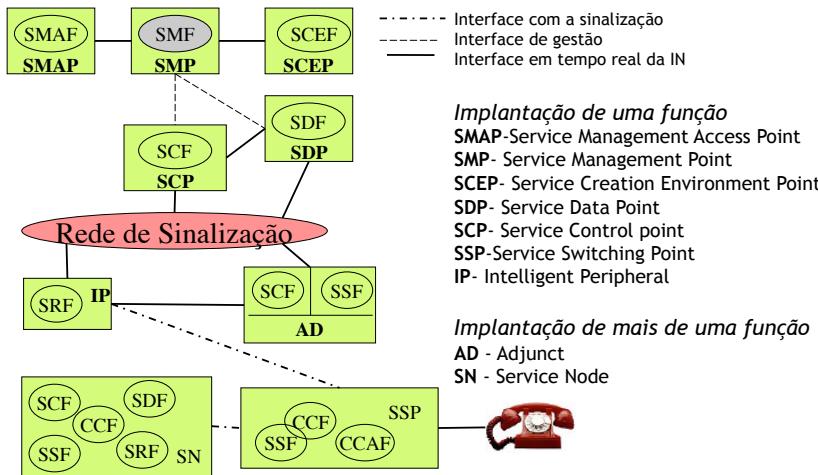


Planos do Modelo Conceptual da Rede Inteligente

- Plano físico (Physical Plane)**
 - Descrição da implantação das entidades funcionais em entidades físicas: *arquitectura física da rede inteligente*
 - A implantação respeita a regra que uma entidade funcional não pode ser repartida por várias entidades físicas. (Pode sim ser duplicada em diferentes entidades físicas)
 - Uma entidade física pode conter várias entidades funcionais desde que sejam de tipo diferente
 - Identifica os diferentes componentes, entidades físicas (*Physical Entities*), e os protocolos que existem entre eles
 - Diferentes tipos de implantação são possíveis
 - A partir de uma arquitectura funcional as escolhas de implementação podem conduzir a diversas arquitecturas físicas
 - Diferentes arquitecturas correspondem usualmente cenários de diferente complexidade (i.e., operador de grande escala vs. pequeno operador).
- Balanço entre escalabilidade/desempenho, complexidade e custo

Planos do Modelo Conceptual da Rede Inteligente

- Arquitectura física (*Physical Plane Architecture(s)*)



Planos do Modelo Conceptual da Rede Inteligente

Arquitectura física: Controlo da chamada e ligação

- **SSP-Service Switching Point:** é um comutador de IN e implementa no mínimo as entidades SSF e CCF. Se for local implementa a entidade CCAF. Se integrar um SCF designa-se por *SSCP-Service Switching and Control Point*
- **IP- Intelligent Peripheral:** contem recursos especializados que não se encontram num SSP, implementa o SRF

Arquitectura física: Multielementos

- **AD - Adjunct:** é um SCP directamente ligado ao SSP que permite melhorar os tempos de resposta.
- **SN-Service Node:** implementa as principais funções da IN: SCF,SDF,SRF e SSF/CCF (Arquitectura usualmente adoptada por pequenos fornecedores de serviços)

Planos do Modelo Conceptual da Rede Inteligente

Arquitectura física: Gestão

- **SMAP- Service Management Access Point:** fornece um acesso ao SMP por um lado aos gestores dos serviços para fins de exploração comercial destes e por outro lado aos utilizadores para permitir modificar os dados do serviço. Implementa a entidade SMAF.
- **SMP- Service Management Point:** responsável pela gestão do serviço e dos SCP associados. As suas funções são: gestão da base de dados, monitorização e teste da rede, gestão do tráfego. Implementa a entidade SMF (eventualmente pode ainda implementar a SMAF e SCEF).
- **SCEP- Service Creation Environment Point:** implementa um SCEF e interage directamente com o SMP.

Arquitectura física: Controlo do serviço

- **SCP- Service Control Point:** é o servidor responsável pelo tratamento dos serviços de IN. Funciona em tempo real acede aos dados e comanda os SSPs. Implementa a entidade SCF (eventualmente pode também implementar o SDF).
- **SDP: Service Data Point:** gera e armazena os dados usados pelo SCP para fornecer os serviços. Implementa a entidade SDF. Accede ao SCP quer directamente quer através da sinalização

Planos do Modelo Conceptual da Rede Inteligente

Relação entre os diferentes planos

- Os serviços apresentados aos utilizadores pela sua descrição no plano dos serviços são criados por um projectista através da interface de programação (no plano funcional global).
 - A criação consiste na definição duma lógica global de serviço, resultando na associação duma cadeia de SIBs (incluindo o BCP) e dos pontos de início e de retorno.
- Cada SIB do plano funcional global é representado no plano funcional repartido através de acções (FEAs) de uma ou mais entidades funcionais.
- As lógicas de serviço global correspondem uma ou mais lógicas de serviço repartidas.
- As relações entre entidades funcionais identificadas na arquitectura funcional são especificadas pelos protocolos no plano físico.

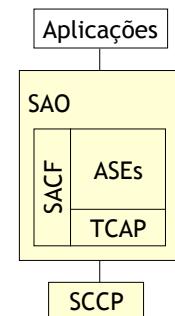
Plano físico para o CS-1

- O plano físico identifica as entidades físicas que implementam as entidades funcionais e os protocolos que permitem a troca de informação entre as entidades físicas.
- As relações existentes entre as entidades funcionais são:
 - SCF-SSF (D)
 - SCF-SRF (E)
 - SCF-SDF (F)

- São relações do tipo pergunta-resposta ou notificação
- Quando as entidades funcionais se encontram implantadas em entidades físicas distintas o fluxo de informação definido no plano funcional repartido é implementado no plano físico pelo protocolo de aplicação de rede inteligente: *INAP (Intelligent Network Application Protocol)*.
- O INAP utiliza para o seu transporte o SS7, sendo as suas mensagens encapsuladas em mensagens do protocolo *TCAP (Transaction Capabilities Application Protocol)*

Plano físico para o CS-1

- Uma entidade física pode ter uma interacção única ou múltipla coordenada com outras entidades físicas.
- ASE- Application Service Element, é definido como um conjunto de funções de aplicação que fornecem as capacidades de interoperação das evocações das entidades de aplicação com uma dada finalidade.
- SAO- Single Association Object, é um conjunto de ASEs com o seu SACF.
- SACF- Single Association Control Function, coordena a utilização do conjunto das ASEs.
- TCAP- Transaction Capability Application Part.
- SCCP: Signalling Connection Control Part do SS7.
- O protocolo ROSE, Remote Operations Services Element é usado com uma ASEs.



Características do CS-2 (1)

- Definido ao mesmo tempo que decorriam:
 - Normalização GSM
 - Desenvolvimento da Internet
 - Abertura dos mercados de telecomunicações
- Três tipos de serviços são considerados:
 - Os serviços de telecomunicações (melhoria do CS-1)
 - Os serviços de gestão (**novidade**)
 - Os serviços de criação (**novidade**)

Características do CS-2 (2)

- Limitações do CS-1:
 - A rede é controlada por um único operador
 - Consideradas apenas serviços de conversas telefónicas *ponto-a-ponto*
 - Não suporta convenientemente comunicações multiponto e multimedia
 - Interacções do utilizador podem apenas ocorrer quando uma chamada está estabelecida.
 - Problemático para os serviços nas redes móveis (e.g., autenticação, localização)
- Requisitos / alterações trazidas pelo CS-2:
 - A rede é controlada por um único operador
 - Mas são possíveis as interacções entre vários SCFs e SDFs
 - Considerados serviços multiparticipantes, *multiponto*
 - O SCF pode controlar mais do que um BCSM simultaneamente
 - Interacções do utilizador podem ocorrer fora do contexto de uma chamada
 - Definição de um novo modelo de estados o BCUSM
 - Utilização de canais extra para além dos canais da chamada
 - Generalização do contexto de criação de serviços.
 - Redefinição do conceito de SIB - recursividade
 - Melhores especificações em termos de: Gestão dos serviços e Interacção de serviços
 - Compatibilidade com o CS-1 (*backwards*)

Plano de serviços do CS-2 (1)

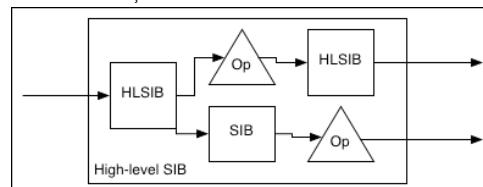
- Os serviços de telecomunicações:
 - Permitem tratar serviços com mais de 2 interlocutores.
 - *Call Party Handling*
 - Permitem ter serviços que são activados/controlados fora do contexto de uma chamada (ex. Autenticação, registo, envio de mensagens).
 - Permitem a internacionalização de serviços (nº verde) devido a existência de mecanismos de interfuncionamento entre vários operadores para fornecer o serviço
- É introduzida o aspecto da mobilidade nos serviços:
 - A mobilidade pessoal fornecida pelo serviço Universal Personal Telecommunication; UTP.
 - A mobilidade dos terminais fornecida pelas redes móveis definindo aspectos da sistemas móveis de terceira geração (a finalizar no CS-3)

Características do CS-2 (2)

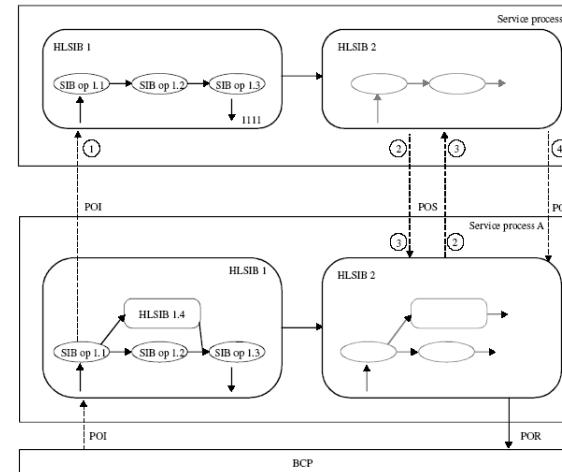
- Os serviços de gestão :
 - Estes serviços são principalmente oferecidos aos assinantes para controlar os seus terminais, através do SMAF, estes podem ser serviços de:
 - controlo permanente que permitem modificar os parâmetros do terminal e dos serviços.
 - monitorização que permitem obter informação sobre os aparelhos e sua utilização.
- Os serviços de criação
 - O CS-2 identifica 3 etapas na criação de serviços às quais estão associadas um conjunto de serviços:
 - *Serviços de especificação* que permite ao projectista efectuar a análise das necessidades com base em estudos de mercado, estudos de eventuais interacções com serviços já existentes e através de uma concepção de alto nível recensear as necessidades em termos de componentes de serviço.
 - *Serviços de desenvolvimento* que permitem conceber de uma forma detalhada o serviço pela definição da lógica de serviço e do esquema de dados e do desenvolvimento dos módulos necessários.
 - *Serviços de verificação* que permitem validar o resultado do desenvolvimento por simulação, teste e entrega do serviço
 - Estas tarefas são efectuadas pela função SCEF- Service Creation Environment Function. Uma vez desenvolvido o novo serviço esta interage com SMF encarregue da disponibilização do serviço na rede e é colocado à disposição.
 - O CS-2 disponibiliza um guia para a criação de serviços e introduz o conceito de gabinete de criação de serviços através da função SCEF.

Plano Funcional Global do CS-2

- Introdução de novos POI e POR no BCP. Definição de POSS.
 - POI durante a chamada (suporte a interacções durante a chamada)
 - POR relacionados com a gestão de ligações em chamadas multiparticipante *Call-Party Handling*
- Introdução de novas SIB
 - O *Basic Call-Unrelated Process (BCUP)*
 - Descrição de interacções do utilizador fora do contexto de uma chamada
 - Exemplo: registo/autenticação de um utilizador
 - Para *Call-Party Handling*: adição (*Join*) e remoção (*Split*) de participantes na chamada
 - Process Management*: gestão da criação e destruição de processos paralelos
- Redefinição do conceito de SIB
 - Modelo recursivo para as SIB
 - Operação de SIB: operação atómica, indivisível (Op)
 - SIB de alto nível, composta por outras SIB (HLSIB)
 - Paralelismo e sincronização entre SIB



Plano Funcional Global do CS-2



- Service process:** combinação de SIBs ou HLSIBs que representam uma actividade no serviço (ex. autorização via PIN).
- Um processo de serviço pode lançar outros processos paralelos ①.
- Sincronização entre processos, durante o processo ②, ③ indicando o fim do processo ④.
- Definição de Points of Synchronization (POS)

Plano Funcional Global do CS-2: SIBs

- ALGORITHM;
- AUTHENTICATE;
- CHARGE;
- COMPARE;
- DISTRIBUTION;
- END;**
- INITIATE SERVICE PROCESS;**
- JOIN;**
- LOG CALL INFORMATION;
- MESSAGE HANDLER;**
- QUEUE** (Duas operações *Queue_Call* e *Queue_Monitor*)
- SCREEN;
- SERVICE DATA MANAGEMENT;
- SERVICE FILTER** (correspondente a *LIMIT* no CS-1)
- SPLIT;**
- STATUS NOTIFICATION;
- TRANSLATE;
- USER INTERACTION;
- VERIFY;
- BASIC CALL PROCESS (BCP);
- BASIC CALL UNRELATED PROCESS (BCUP)**

Algumas novas SIBs e redefinição de outras já presentes no CS-1

Plano Funcional Global do CS-2: SIBs

SIBs para suporte a processos de serviço paralelos

- INITIATE SERVICE PROCESS**
Inicia a execução de um novo processo de serviço paralelo
- MESSAGE HANDLER**
Troca de mensagens entre processos de serviço paralelos.
Esta SIB possui dois tipos de operações (enviar e receber mensagens).
- END**
Indica o fim da execução de um processo de serviço

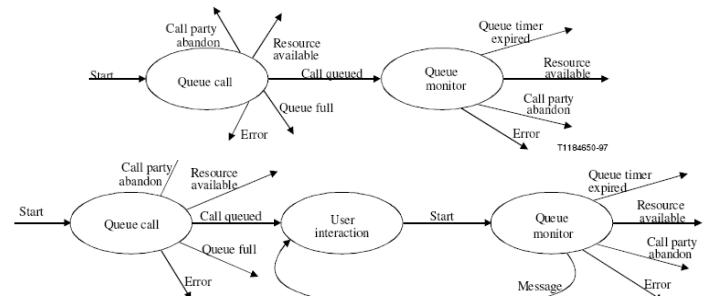
SIBs para suporte ao *Call Party Handling (CPH)*

- JOIN**
Junta um participante (ou grupo de participantes) numa chamada a outro grupo de participantes na mesma chamada
- SPLIT**
Separa um participante (ou grupo de participantes) da chamada corrente e coloca-a(as) numa nova chamada ou noutra chamada já existente

Plano Funcional Global do CS-2: SIBs

• QUEUE

Duas operações distintas: colocar o participante numa fila (Queue Call) e monitorizar o estado na fila (Queue Monitor)



Plano Funcional Global do CS-2: BCUP

• BASIC CALL UNRELATED PROCESS (BCUP)

SIB especial (tal como a BCP) para suporte de serviços (ou elementos de serviço) fora do contexto de uma chamada (*call unrelated*)
(Ex. registo de utilizador, envio de mensagens.)

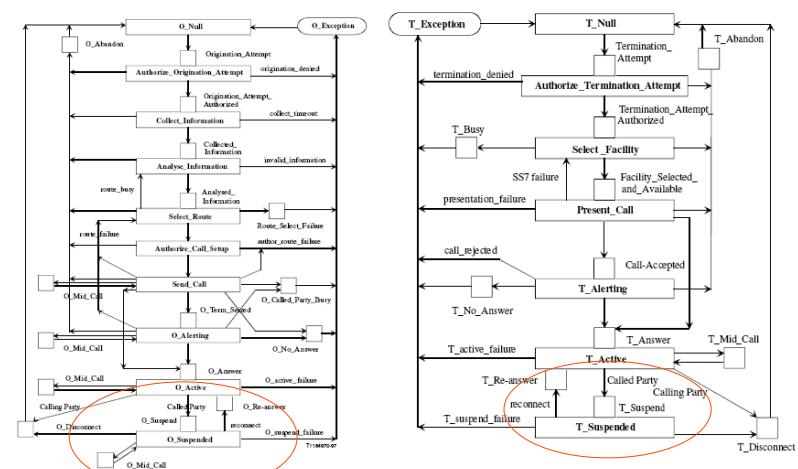
POI	POS (POR)
Analyzed message	Continue with existing data
Answer	Proceed with new data
Release association requested	Release association
	Initiate association

Plano Funcional Repartido do CS-2 (1)

- Introdução de novas Entidades Funcionais
 - Call-Unrelated Service Function - CUSF: processamento de acontecimentos do utilizador não associados com chamadas
 - Service Control User Agent Function - SCUAF: interface/representação para o utilizador interagir com o CUSF
 - Service Management Access Function - SMAF: interface para acesso externo à SMF (ex., via Internet)
 - Intelligent Access Function - IAF: permite a interacção entre o SCF com equipamento não-IN
 - Funções para as redes móveis:
 - Call-related Radio Access Control Function - CRACF
 - Call-unrelated Radio Access Control Function - CURACF
 - Radio Control Function - RCF
- Definição de novos fluxos de informação entre as FE
 - Comunicação entre SCFs e SDFs
 - Distribuição dos SCF e dos SDF
 - Exemplo: International Virtual Private Network (IVPN)
- Introdução de novos DP e PIC
 - Ex. O PIC O_T_Suspended (chamada em suspenso)

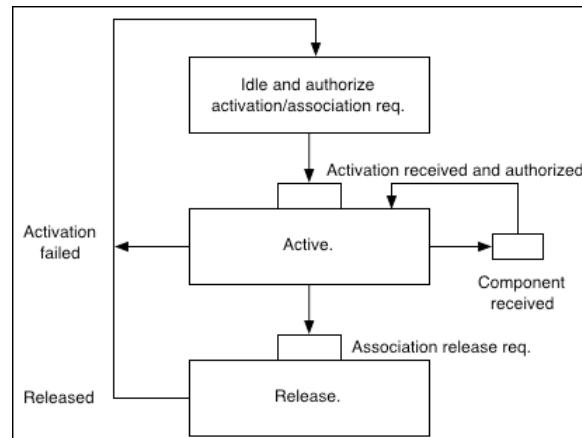
Plano Funcional Repartido do CS-2 (2)

- Modificações no O/T BSCM (suporte a acções no meio da chamada)



Plano Funcional Repartido do CS-2 (2.1)

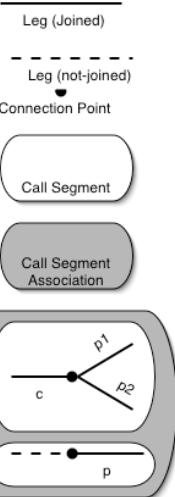
- Introdução do *Basic Call-Unrelated State Model - BCUSM*



Plano Funcional Repartido do CS-2 (3): CV

Motivação: Introdução do *Connection Party Handling (CPH)*

- Controlo dos múltiplos participantes e ligações numa chamada
- Definição de um modelo formal para descrição do estado das ligações numa chamada: *Connection View - CV*
- Principais elementos do CV: Objectos CV
 - Call Segment - CS*: Descrita em termos de *CPs* e *Legs*
 - Connection Point - CP*: uma junção entre duas ou mais *Legs* (uma *Leg* tem de ser obrigatoriamente *controlling*)
 - Leg*: parte do troço de comunicação entre participantes numa chamada.
 - Dois tipos:
 - Controlling* (onde se invoca a lógica de serviço) ou *Passive*.
 - Caracterizadas por estados:
 - Joined*: estado estável em que a *Leg* se encontra ligada ao *Connection Point*
 - Shared (controlling leg)*: não pertence a este CS mas a um CS associado
 - Pending*: a chamada ainda se encontra em estabelecimento
 - Surrogate (controlling leg)*: participação na chamada mas não nas ligações (ex. alguém que encaminhou uma chamada)
 - Call Segment Association - CSA*: grupo de CSs envolvidos num serviço e controlados pelo SCF.
 - (Uma chamada com 2 participantes têm 2 CSAs: um para o chamador e outra para o chamado).



Plano Funcional Repartido do CS-2 (4)

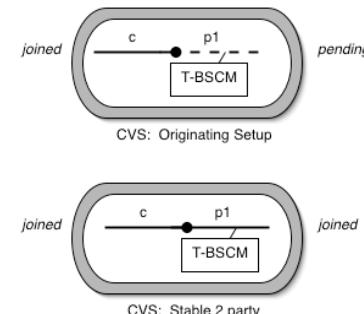
Operações atómicas nos Objectos CV

- Leg**
 - MoveLeg**: de um CS para outro CS associado
 - SplitLeg**: cria um novo CS no CSA movendo para lá esta Leg
 - DisconnectLeg**: liberta os recursos associados a esta Leg
- Call Segment**
 - MergeCallSegment**: une dois CS associados
 - MoveCallSegment**: move um CS de um CSA para outro
- Call Segment Association**
 - CreateCallSegmentAssociation**: cria uma nova CSA

Plano Funcional Repartido do CS-2 (4.1)

- Exemplo usando o *Connection View Model*:
Serviço de chamada em espera com multiparticipantes:

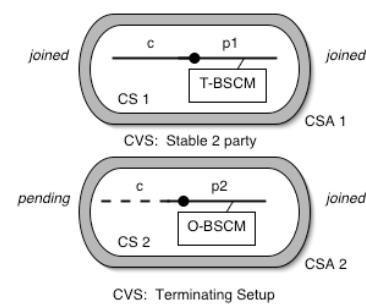
- Um utilizador quando numa chamada é avisado que outro lhe está a tentar ligar.
- Este utilizador tendo a possibilidade de antender esta chamada, sendo o utilizador suspenso avisado desse facto.
- Através do teclado do telefone pode ser selecionado falar com apenas 1 ou todos os outros utilizadores



- Um utilizador tenta uma chamada para um outro
- A chamada é antendida

Plano Funcional Repartido do CS-2 (4.2)

- Exemplo usando o *Connection View Model* (cont.):



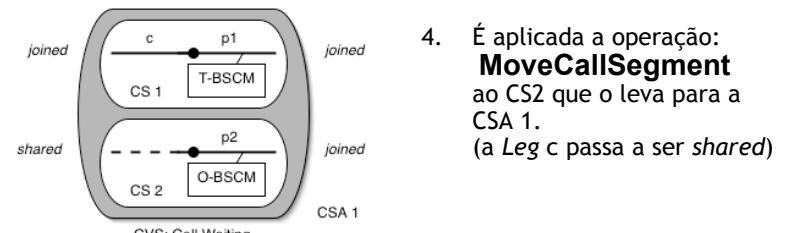
3. Um terceiro utilizador tenta uma chamada para um dos outros utilizadores.

É activado o serviço através do disparo do trigger armado no DP "T_Busy" (no O-BSCM de p2)

(a *Leg controlling* é a do chamado uma vez que é o seu estado que vai iniciar o serviço).

Plano Funcional Repartido do CS-2 (4.3)

- Exemplo usando o *Connection View Model* (cont.):



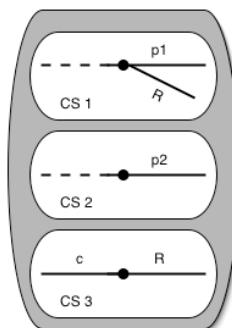
4. É aplicada a operação: **MoveCallSegment** ao CS2 que o leva para a CSA 1.
(a *Leg c* passa a ser *shared*)

5. O utilizador da *Leg c* é avisado e decide atender a chamada em espera, aplicando a operação: **MoveLeg**

Entretanto a *Leg p1* é ligada a outra *Leg R* para ouvir um anúncio que foi suspenso.

Plano Funcional Repartido do CS-2 (4.4)

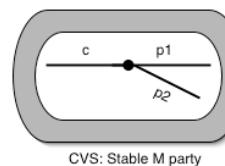
- Exemplo usando o *Connection View Model* (cont.):



6. O utilizador carrega nas molas (*hook flash*) do telefone e dá início a uma *User Interaction*. É aplicada a operação **SplitLeg** na *Leg c* que cria uma nova CS (CS3) movendo para lá a *Leg c* que liga a uma *Leg* para um recurso especial *R*.

Plano Funcional Repartido do CS-2 (4.5)

- Exemplo usando o *Connection View Model* (cont.):



7. Na *User Interaction* o utilizador selecciona falar com todos os outros utilizadores. São libertados os recursos associados às *Legs* de recursos especiais, com a operação **DisconnectLeg**

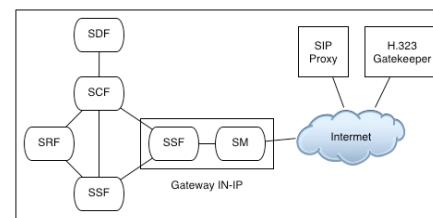
Todas as *Legs* são ligadas ao mesmo CP com a operação **MergeCallSegment**

Características do CS-3

- Novas funcionalidades introduzidas pelo CS-3
 - Portabilidade de números
- Alterações introduzidas em 1999 no CS-3
 - Q.1234 Modelos para o Edge View e Leg View (separação do CV)
 - Apresenta os novos documentos:
 - Q.1236 Modelo de alto nível para a gestão de informação
 - Q.1237 Descrição do suporte do CS-3 para a RDIS de banda-larga
 - Q.1238 Redefinição do INAP
- Melhoramentos introduzidos pelo ETSI ao CS-2 e CS-3
 - Acção de normalização da IN: Services and Protocols for Advanced Networks Group 3 - SPAN 3
 - Resultante das dificuldades em implementar a IN
 - Exemplo: várias versões do INAP
 - Solução ETSI: definição do *Core INAP*
 - Especificação de todo o DFP para o CS-2 e CS-3
 - Utilizando a linguagem formal Service Description Language - SDL (ITU-T)
 - Utilizando máquinas de estados
 - Utilizada para a especificação, simulação e validação de serviços
 - Definição de conjuntos de testes para as implementações IN:
 - Protocol Implementation Conformance Statements (PICS)

Características do CS-4

- Adiamento na prática até ao CS-4 (2001) de:
 - Suporte e integracção com a Internet
 - A alteração mais significativa
 - Suporte e integracção com as redes móveis
 - Maior suporte para comunicações multimédia
- No CS-4 são apresentadas:
 - Alterações significativas ao INAP (Q.1248)
 - Alterações ao DFP (Q.1244)
- Suporte e integracção com a Internet



- *Propostas do IETF*
- *PINT*
 - Estabelecimento de chamadas a partir da Web
- *SPIRITS*
 - Protocolo para o serviço: *call waiting*

Pontos fracos das Redes Inteligentes

Característica	Ponto fraco / solução proposta
Controlo Centralizado dos serviços	Problema de capacidade - <i>mais que um SCP</i> Fiabilidade do SCP - <i>mais que um SCP</i> Fiabilidade das ligações com o SCP- <i>ligações redundantes</i>
Rápida implementação e personalização dos serviços	Muito rápida entrada em serviço Serviços que se sobrepõem - <i>entrada em serviço em áreas restritas para teste</i> . Várias variantes do mesmo serviço. Interacção entre serviços. - Teste, limitar essas interacções
Controlo remoto dos serviços	Controlo complicado O utilizador pode alterar parâmetros e provocar danos - <i>acesso restrito</i> Segurança controlo de utilizador - <i>monitorização</i> Fraude
Expansão em áreas de negócios que beneficiam dos serviços de Telecomunicações	Necessidade de aumento de fiabilidade As empresas depositam maior confiança nas telecomunicações e esperam que esta não falhe. Publicidade, atendimento a clientes etc.

Desafios para as Redes Inteligentes

Um objectivo

- *Aumentar o número de chamadas com sucesso.*
 - A linha está ocupada
 - call waiting, call completion to busy subscriber, fax,...
 - O destinatário não atende (As pessoas movem-se cada vez mais: casa, trabalho)
 - call completion when no replay, fax, voice message,...
 - Existe congestão na rede, melhor gestão, melhores redes, prioridades
 - Erro de marcação - melhor interface, marcação abreviada
 - Atende a pessoa errada, toques pessoais, cartões personalizados.

Algumas pistas

- Uma maior variedade de serviços
- Pacotes de serviços adequados a cada negócio.
- Serviços globais e locais
- Aumento da mobilidade
- Aumento do uso das comunicações diferidas
- Aumento do uso de terminais móveis
- Aumento da segurança e da fiabilidade
- Aumento da procura de serviços identificados
- Aumento do uso dos cartões
- Crescente uso de serviços simples e de interface simples
- Uso de serviços de banda larga e estreita
- Aumento de serviços multimédia

B.2 Descriptions of targeted service features

B.2.1 Abbreviated dialling (ABD)

B.2.1.1 Description No. 1

This feature allows the definition of abbreviated dialling numbers with a VPN. For the users of the VPN, the abbreviated dialling numbers are not subjected to call restrictions, e.g. a VPN user may not be allowed to access the Off-net Calling service feature but can reach an off-net number via this feature.

B.2.1.2 Description No. 2

This feature allows the definition of abbreviated dialling digit sequences to represent the actual dialling digit sequence, i.e., a two digit sequence may represent a complete dialling sequence for a private or public numbering plan.

B.2.1.3 Description No. 3

This service feature is an originating line feature that allows business subscribers to dial others in their company using a short numbering, even if the calling user's line and the called user's line are served by different switches.

B.2.2 Attendant (ATT)

This service feature allows VPN users to access an attendant position within the VPN for providing VPN service information (e.g. VPN numbers). The attendant(s) can be accessed by dialling a special access code.

B.2.3 Authentication (AUTC)

This service feature allows for the verification that a user is allowed to exercise certain options in a telephone network. In other words, the request made by the user is authentic and should be granted.

B.2.4 Authorization code (AUTZ)

This service feature allows a VPN user to override calling restrictions of the VPN station from which the call is made. Different sets of calling privileges can be assigned to different authorization codes and a given authorization code can be shared by multiple users.

B.2.5 Automatic call back (ACB)

This service feature allows the called party to automatically call back the calling party of the last call directed to the called party.

B.2.6 Call distribution (CD)

This service feature allows the served user to specify the percentage of calls to be distributed among two or more destinations. Other criteria may also apply to the distribution of calls to each destination.

B.2.7 Call forwarding (CF)

This service feature allows the user to have his incoming calls addressed to another number, no matter what the called party line status may be.

B.2.8 Call forwarding on busy/don't answer (CFC)

This service feature allows the called user to forward particular calls if the called user is busy or does not answer within a specified number of rings.

B.2.9 Call gapping (GAP)

B.2.9.1 Description No. 1

This service feature allows the service provider to automatically restrict the number of calls to be routed to the subscriber.

B.2.9.2 Description No. 2

This service feature allows to restrict the number of calls to a served user to prevent congestion of the network.

B.2.10 Call hold with announcement (CHA)

The call hold with announcement service feature allows a subscriber to place a call on hold with options to play music or customized announcements to the held party.

B.2.11 Call limiter (LIM)

B.2.11.1 Description No. 1

This service feature allows a served user to specify the maximum number of simultaneous calls to a served user's destination. If the destination is busy, the call may be routed to an alternative destination.

B.2.11.2 Description No. 2

This service feature enables to count the running calls to the subscriber and to reject all the new calls when a threshold of simultaneous calls is reached. As an option, this threshold may be real-time managed by the subscriber.

Associated with call volume distribution or call distribution, it allows the rerouting of the new calls.

B.2.12 Call logging (LOG)

This service feature allows for a record to be prepared each time that a call is received to a specified telephone number.

B.2.13 Call queueing (QUE)

B.2.13.1 Description No. 1

This service feature allows a served user to have calls meeting busy at the scheduled destination to be placed in a queue and connected as soon as free condition is detected. Upon entering the queue, the caller hears an initial announcement informing the caller that the call will be answered when a line is available.

B.2.13.2 Description No. 2

This service feature enables the subscriber, when a call encounters a terminating trigger such as a busy condition or a specified number of rings to queue that call, a specific announcement being sent to the calling party.

B.2.14 Call transfer (TRA)

The call transfer service feature allows a subscriber to place a call on hold and transfer the call to another location.

B.2.15 Call waiting (CW)

This service feature allows the called party to receive a notification that another party is trying to reach his number while he is busy talking to another calling party.

B.2.16 Closed user group (CUG)

This service feature allows the user to be a member of a set of VPN users who are normally authorized to make and/or receive calls only within the group. A user can belong to more than one CUG. In this way, a CUG can be defined so that certain users are allowed either to make calls outside the CUG, or to receive calls from outside the CUG, or both.

B.2.17 Consultation calling (COC)

The consultation calling service feature allows a subscriber to place a call on hold, in order to initiate a new call for consultation.

B.2.18 Customer profile management (CPM)

This service feature allows the subscriber to real-time manage his service profile, i.e., terminating destinations, announcements to be played, call distribution, and so on.

B.2.19 Customized recorded announcement (CRA)

This service feature allows a call to be completed to a (customized) terminating announcement instead of a subscriber line. The served user may define different announcements for unsuccessful call completions due to different reasons (e.g. caller outside business hours, all lines are busy).

B.2.20 Customized ringing (CRG)

This service feature allows the subscriber to allocate a distinctive ringing to a list of calling parties.

B.2.21 Destinating user prompter (DUP)

This service feature enables to prompt the called party with a specific announcement. Such an announcement may ask the called party to enter an extra numbering, e.g. through dual-tone multi-frequency (DTMF), or a voice instruction that can be used by the service logic to continue to process the call.

B.2.22 Follow-me diversion (FMD)

B.2.22.1 Description No. 1

This service feature allows a VPN user to change the routing number of his/her VPN code via a DTMF phone. The updated number can be another VPN code or a PSTN number.

B.2.22.2 Description No. 2

With this service feature, a user may register for incoming calls to any terminal access. When registered, all incoming calls to the user will be presented to this terminal access. A registration for incoming calls will cancel any previous registration. Several users may register for incoming calls to the same terminal access simultaneously. The user may also explicitly deregister for incoming calls.

B.2.23 Mass calling (MAS)

This service feature allows processing of huge numbers of incoming calls, generated by broadcasted advertisements or games.

B.2.24 Meet-me conference (MMC)

This service feature allows the user to reserve a conference resource for making a multi-party call, indicating the date, time, and conference duration. At the specified date and time, each participant in the conference has to dial a designated number which has been assigned to the reserved conference resource, in order to have access to that resource, and therefore, the conference.

B.2.25 Multiway calling (MWC)

This service feature allows the user to establish multiple, simultaneous telephone calls with other parties.

B.2.26 Off-net access (OFA)

This service feature allows a VPN user to access his or her VPN from any non-VPN station in the PSTN by using a personal identification number (PIN). Different sets of calling privileges can be assigned to different PINs, and a given PIN can be shared by multiple users.

B.2.27 Off-net calling (ONC)

This service feature allows the user to call outside the VPN network. Calls from one VPN to another are also considered off-net.

B.2.28 One number (ONE)

This feature allows a subscriber with two or more terminating lines in any number of locations to have a single telephone number. This allows businesses to advertise just one telephone number throughout their market area and to maintain their operations in different locations to maximize efficiency. The subscriber can specify which calls are to be terminated on which terminating lines based on the area the calls originate.

B.2.29 Origin dependent routing (ODR)

This service feature enables the subscriber to accept or reject a call, and in case of acceptance, to route this call, according to the calling party geographical location. This service feature allows the served user to specify the destination installation(s) according to the geographical area from which the call was originated.

B.2.30 Originating call screening (OCS)

This service feature allows the served user to bar calls from certain areas based on the District code of the area from which the call is originated.

B.2.31 Originating user prompter (OUP)

B.2.31.1 Description No. 1

This service feature allows a served user to provide an announcement which will request the caller to enter a digit or series of digits via a dual-tone multi-frequency (DTMF) phone or generator. The collected digits will provide additional information that can be used for direct routing or as a security check during call processing.

B.2.31.2 Description No. 2

This service feature enables to prompt the calling party with a specific announcement. Such an announcement may ask the calling party to enter an extra numbering (e.g. through DTMF) or a voice instruction that can be used by the service logic to continue to process the call.

B.2.32 Personal numbering (PN)

This service feature supports a UPT number that uniquely identifies each UPT user and is used by the caller to reach that UPT user. A UPT user may have more than one UPT number for different applications (e.g. a business UPT number for business calls and a private UPT number for private calls), however, a UPT user will have only one UPT number per charging account.

B.2.33 Premium charging (PRMC)

This service feature allows for the pay back of the part of the cost of a call to the called party, when he is considered as a value added service provider.

B.2.34 Private numbering plan (PNP)

This service feature allows the subscriber to maintain a numbering plan within his private network, which is separate from the public numbering plan.

NOTE – See also definition under VPN description.

B.2.35 Reverse charging (REVC)

This service feature allows the service subscriber (e.g. freephone) to accept to receive calls at its expense and be charged for the entire cost of the call.

B.2.36 Split charging (SPLC)

This service feature allows for the separation of charges for a specific call, the calling and called party each being charged for one part of the call.

B.2.37 Terminating call screening (TCS)

This service feature allows the user to screen calls based on the terminating telephone number dialled.

B.2.38 Time dependent routing (TDR)

B.2.38.1 Description No. 1

This service feature enables the subscriber to accept or reject a call, and in case of acceptance, to route this call, according to the time, the day in the week and the date.

B.2.38.2 Description No. 2

This service feature allows the served user to apply different call treatments based on time of day, day of week, day of year, holiday, etc.

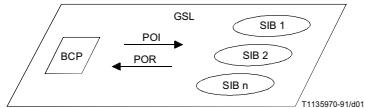


FIGURE 1/Q.1213
Global functional plane model

5 IN CS-1 Service Independent Building Blocks (SIBs)

The following list of SIBs have been identified as required to support the list of targeted IN CS-1 services and service features identified in Recommendation Q.1211 [3]:

- ALGORITHM
- AUTHENTICATE
- CHARGE
- COMPARE
- DISTRIBUTION
- LIMIT
- LOG CALL INFORMATION
- QUEUE
- SCREEN
- SERVICE DATA MANAGEMENT
- STATUS NOTIFICATION
- TRANSLATE
- USER INTERACTION
- VERIFY

The stage 1 SIB descriptions that follow reflect the understanding of the logical function of each SIB in its role of supporting IN CS-1 services and service features. The BCP, which is viewed as a specialized SIB, is described in clause 6.

An explanation of the format of the stage 1 SIB descriptions is outlined below.

5.1 Data parameters for SIBs

By definition, SIBs are independent of the service/SF they are used to represent. They have no knowledge about previous or subsequent SIBs which are used to describe the service feature.

In order to describe service features with these generic SIBs, some elements of service dependence is needed. Service dependence can be described using data parameters which enable a SIB to be tailored to perform the desired functionality. Data parameters are specified independently for each SIB and are made available to the SIB through global service logic.

Two types of data parameters are required for each SIB, dynamic parameters called Call Instance Data (CID) and static parameters called Service Support Data (SSD).

Recommendation Q.1213 (10/95) 3

5.2.2 Operation

Description of actions performed by the SIB. The operations section expands on the definition, to allow the reader to clearly understand the operation that this SIB is intended to perform.

5.2.3 Potential service applications

Service examples of where this SIB can be used.

5.2.4 Input

Input to each SIB is specified as three distinct elements:

- one logical start;
- Service Support Data which defines parameters which are specified by the service description;
- Call Instance Data which are specific to that call instance.

5.2.5 Output

Output from each SIB is specified as two distinct elements:

- one or more logical end;
- call instance data which defines data parameters specific to that call instance which results from the execution of that SIB and are required by other SIBs or the BCP to complete the call service instance.

5.2.6 Graphic representation

A graphic representation is used to describe input, operations and output of the SIB and is illustrated in Figure 2. Each SIB is characterized by having one logical start and one or more logical ends. These logic flows are shown by the solid arrows on the left and right of the diagram. Each logic flow is specified above each arrow. SSD parameters are identified by the dashed arrow at the top of the diagram and are specified beside the dashed arrow. Similarly, CID parameters are specified below the diagram. Input CID parameters are separated from the output parameters.

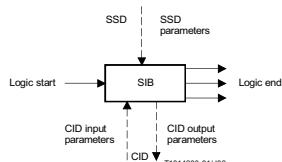


FIGURE 2/Q.1213
Graphical representation of IN CS-1 SIB

5.2.7 SDL diagram

This diagram gives a graphic representation of the stage 1 description of the SIB using SDL macro diagrams (see Recommendation Z.100 [6]).

Recommendation Q.1213 (10/95) 5

5.1.1 Call Instance Data (CID)

Call instance data defines dynamic parameters whose value will change with each call instance. They are used to specify subscriber specific details like calling or called line information. This data can be:

- made available from the BCP SIB (e.g. Calling Line Identification);
- generated by a SIB (e.g. a translated number); or
- entered by the subscriber (e.g. a dialled number or a PIN code).

Associated with each CID value is a logical name which is referred to as the CID Field Pointer (CIDFP). If a SIB requires CID to perform its function, there will be an associated CIDFP assigned through SSD (refer to 5.1.2). For instance, the TRANSLATE SIB's CID which defines what is to be translated is called Information. The TRANSLATE SIB's SSD parameter which defines where this data can be found is CIDFP-Filter Value(s).

Since the CID value can vary with each call instance, service features can be written with data flexibility. In the above TRANSLATE SIB example, one service feature may require translation of a calling number, while another service feature will require translation of the called number. In both cases, the data required by the SIB is specified by the information Calling Line Identity (CLI), but the CIDFP-Filter Value(s) changes. In the first service feature, the value of CIDFP-Filter Value(s) is set to CLI, while the second service feature sets the value of CIDFP-Filter Value(s) to Called Number.

Once a CIDFP has been specified for a service feature, it can be referenced by subsequent SIBs, and the CID value can be made available to all subsequent SIBs in the SIB chain. This CIDFP is said to be fixed for that service and is constant for all instances of that service. The actual value of the CID changes for each call instance of that service feature.

5.1.2 Service Support Data (SSD)

Service support data defines data parameters required by a SIB which are specific to the service feature description. When a SIB is included in the GSL of a service description, the GSL will specify the SSD values for the SIB. SSD consists of:

i) Fixed parameters

These are data parameters whose values are fixed for all call instances. For instance, the "File Indicator" SSD for the TRANSLATE SIB needs to be specified uniquely for each occurrence of that SIB in a given service feature. The "File Indicator" SSD value is then said to be fixed, as its value is determined by the service/SF description, not by the call instance.

If a service/SF is described using multiple occurrences of the same SIB, then fixed SSD parameters are defined uniquely for each occurrence.

ii) Field pointers

Field pointers identify which CID is required by the SIB, and in doing so provide a logical location for that data. They are signified by "CIDFP-xxxx", where "xxxx" names the data required. For instance, "CIDFP-Filter Value(s)" for the TRANSLATE SIB will specify which CID element is to be translated.

If more than one CID is required by a SIB to perform its function, then the SSD data parameters will contain multiple field pointers.

5.2 Method to describe IN CS-1 SIBs

The following template applies to characterize and describe the SIBs.

5.2.1 Definition

Prose description of the SIB from the service creation point of view.

4 Recommendation Q.1213 (10/95)

5.3 ALGORITHM

5.3.1 Definition

Applies a mathematical algorithm to data to produce a data result.

5.3.2 Operation

This SIB takes a specified call instance data and applies the specified mathematical algorithm to it to produce the corresponding data result.

It can be used to implement a simple arithmetic operation as incrementing a counter.

5.3.3 Potential service applications

- Mass calling;
- Televoicing.

5.3.4 Input

5.3.4.1 Logical start

Indicates the logical start of execution for the SIB.

5.3.4.2 Service support data

- Type
 - a) increment;
 - b) decrement.
- Value
 - Specifies the amount to be used when applying the SIB (e.g. 1, 2, etc.).
- CIDFP-Data
 - This CID field pointer specifies the call instance data to which the algorithm is to be applied.
- CIDFP-Error
 - This CID field pointer specifies where in output call instance data the error cause will be written.

5.3.4.3 Call instance data

- Data
 - The identifier is the data associated with the CIDFP-Data upon which algorithm is to be applied.

5.3.5 Output

5.3.5.1 Logical end

- Success;
- Error.

5.3.5.2 Call instance data

- Data
 - Contains the resultant value after the SIB has completed.

6 Recommendation Q.1213 (10/95)

- Error cause
Identifies the specific condition which caused an error during the operation of the SIB. The following errors have been identified for ALGORITHM:
 - a) invalid type;
 - b) invalid value.

5.3.6 Graphical representation

See Figure 3.

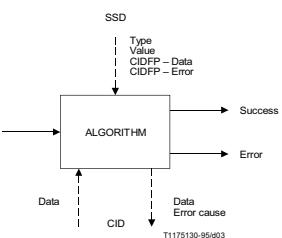


FIGURE 3/Q.1213
ALGORITHM SIB

5.4 AUTHENTICATE

5.4.1 Definition

Provides authentication functionality for a service.

5.4.2 Operation

This SIB provides an authentication function to establish an authorized relationship between the service logic and a database on behalf of a user.

The authentication function can be either simple authentication or externally defined.

5.4.3 Potential service applications

- All services.

5.4.4 Input

5.4.4.1 Logical start

Indicates the logical start of execution for the SIB.

5.4.4.2 Service support data

- Authenticate Name (optional)

This SSD field is only used if SSD Authenticate Mechanism ID has value "Simple". The Authenticate Name is used to identify the location of the object containing the Authenticate Password attribute in order to set up an Authorized Relationship. A "null" in this SSD field indicates that the Authenticate Name can vary and its value must be provided through call instance data.

Recommendation Q.1213 (10/95) 7

- Authenticate Password (optional)

This SSD field is only used if SSD Authenticate Mechanism ID has value "Simple". The Authenticate Password provides the data to be matched in the Authenticate Name object in order to set up an Authorized Relationship. A "null" in this SSD field indicates that the Authenticate Name can vary and its value must be provided through call instance data.

- Authenticate Mechanism Id

The Authenticate Mechanism Id identifies the authentication mechanism which is to be used to establish the Authorized Relationship. It may take one of the following values:

- None, which implies that no authentication is performed.
- Simple, which implies that simple authentication is performed.
- External, which implies that an externally defined authentication is performed.

- CIDFP - Error

This CID field pointer specifies where in output call instance data the error cause will be written.

- CIDFP - Authorized Relationship Id

This CID field pointer specifies where in output call instance data the Authorized Relationship Id will be written.

- CIDFP - Authenticate Name

This CID Field Pointer specifies which call instance data is to be used as the Authenticate Name.

- CIDFP - Authenticate Password

This CID Field Pointer specifies which call instance data is to be used as the Authenticate Password.

5.4.4.3 Call instance data

- Authenticate Name (optional)

This CID field is only used if SSD Authenticate Mechanism Id has value "Simple" and SSD Authenticate Name has value "null". The Authenticate Name is used to identify the location of the object containing the Authenticate Password attribute in order to set up an Authorized Relationship.

- Authenticate Password (optional)

This CID field is only used if SSD Authenticate Mechanism ID has value "Simple" and SSD Authenticate Name has value "null". The Authenticate Password provides the data to be matched in the Authenticate Name object in order to set up an Authorized Relationship.

NOTE - When Authenticate Name and Authenticate Password are supplied as input CID, the SSD parameters Authenticate Name and Authenticate Password are not used.

5.4.5 Output

5.4.5.1 Logical end

- Success (Authentication successful);
- Error.

5.4.5.2 Call instance data

- Error cause

Identifies the specific condition which caused an error during the operation of the SIB.

- Authorized Relationship Id

The Authorized Relationship Id provides the identity of the established Authorized Relationship through which operations can be applied.

8 Recommendation Q.1213 (10/95)

Typically, charging may be directed towards:

- the account identified by the CLI;
- the account identified by the called number (either the dialled number or the destination number);
- an account or credit card identified by the collected user information;
- the calling user's exchange accumulator;
- a payphone.

5.5.3 Potential service application

- Any service which requires specific IN charging.

5.5.4 Input

5.5.4.1 Logical start

Indicates the logical start of execution for the SIB.

5.5.4.2 Service support data

- number of accounts to charge;
- Account.

Each account is specified by two parameters, as follows:

- a) Number

Specifies one of the following:

- 1) CIDFP-Line

This CID field pointer specifies which call instance data is to be used as the line number to charge.

- 2) CIDFP-Account

This CID field pointer specifies which call instance data is to be used as the account number to charge.

- 3) Fixed account

Specifies an account number which is fixed for all call instances.

- b) Per cent (%)

Specifies the allocation of the total charge for this account. The sum of all allocations must equal 100%.

- Resource type

Specifies the resource to be charged for (e.g. bearer type, announcement, SCF usage, etc.).

- Units

Specifies a premium value for the specified resource type.

- Service/service feature identifier

Specifies the service/service feature for which charging is to be applied.

- CIDFP-Pulse

This CID field pointer specifies which call instance data is used to identify pulse metering on the calling line.

- CIDFP-Error

This CID field pointer specifies where in output call instance data the error cause will be written.

5.5 CHARGE

5.5.1 Definition

Determine special charging treatment for the call, where special refers to any charging in addition to that normally performed by the basic call process.

In general, this involves identifying:

- the resources for which charging is to occur;
- to where the charges are to be directed.

It should be noted that this SIB is not responsible for the subscriber billing process.

5.5.2 Operation

The charging information output by this SIB must be compatible with the charging and billing system of the network operator or service provider. However, this SIB does not define the format of the output nor does it identify all the types of information that an Administration will require for charging. Generation of bills will often be done off-line by the Administration's existing billing system.

The CHARGE SIB is used for specific resource charging and may be invoked several times in one service/service feature instance.

Different simultaneous or consecutive call instances may charge the same account.

Typical resources for which charging can occur are:

- circuit-mode bearers;
- packet or messages;
- SRF resources, e.g. announcements, voice message storage, etc.;
- SCF usage (in units).

Recommendation Q.1213 (10/95) 9

10 Recommendation Q.1213 (10/95)

5.5.4.3 Call instance data

- Line(s) Specifies a line number for charging. This can be the calling line, the dialled number or a destination number.
- Account(s) Specifies an account number for charging. This is an account number which was entered during the call such as a credit card or a calling card number.
- Pulse metering When specified, indicates that pulse metering is associated with the calling line.

5.5.5 Output

5.5.5.1 Logical end

- Success;
- Error.

5.5.5.2 Call instance data

- Error cause Identifies the specific condition which caused an error during the operation of the SIB. The following errors have been identified for CHARGE:
 - invalid account to charge;
 - invalid percentage allocation ($> 100, < 0$);
 - invalid sum of percentage allocations (not equal to 100);
 - invalid service/service feature;
 - invalid resource;
 - invalid units;
 - system fault - unable to write record.

5.5.6 Graphical representation

See Figure 5.

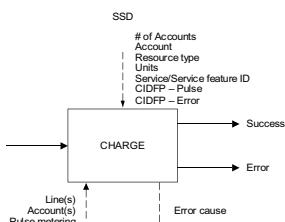


FIGURE 5/Q.1213
CHARGE SIB

Recommendation Q.1213 (10/95) 11

5.6 COMPARE

5.6.1 Definition

Performs a comparison of an identifier against a specified reference value. Three results are possible:

- identifier is GREATER THAN the value;
- identifier is LESS THAN the value;
- identifier is EQUAL TO the value.

5.6.2 Operation

This SIB compares an identifier to a specified reference value. One of three logical ends will result from this operation (e.g. $<$, $>$, or $=$). Other logical ends can be formulated by combining two of the logical ends together (e.g. $<$, \leq , or \geq).

It can be used for:

- Comparing an identifier to a specified reference value. For instance, for checking that the current number of calls is less than the maximum number authorized.
- For checking the relationship of current network time to a customer specified time to perform time dependent decision. The comparison may be done on Time of Day (TOD), Day of Week (DOW), or Day of Year (DOY). The reference value is then the customer specified TOD, DOW or DOY.

5.6.3 Potential service applications

- Time dependent routing;
- CCBS.

5.6.4 Input

5.6.4.1 Logical start

Indicates the logical start of execution for the SIB.

5.6.4.2 Service support data

- Comparison type Specifies the type of comparison to be performed. The following types have been identified:
 - Identifier value – Compare the identifier against the reference value.
 - Time – Compare network time to the reference value. Network time is specified as:
 - time of day;
 - day of week; or
 - day of year.
 - CIDFP-Data This CID field pointer specifies which call instance data is to be used as the identifier.
 - Reference value Specifies the value against which the comparison will be made.
 - CIDFP-Error This CID field pointer specifies where in output call instance data the error cause will be written.

12 Recommendation Q.1213 (10/95)

5.6.4.3 Call instance data

- Data Specifies the data associated with the CIDFP-Data (see SSD) which is to be compared to the reference value.

5.6.5 Output

5.6.5.1 Logical end

- GREATER THAN the value;
- LESS THAN the value;
- EQUAL TO the value;
- Error.

5.6.5.2 Call instance data

- Error cause Identifies the specific condition which caused an error during the operation of the SIB. The following errors have been identified for COMPARE:
 - invalid identifier;
 - invalid reference value.

5.6.6 Graphical representation

See Figure 6.

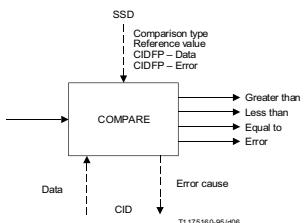


FIGURE 6/Q.1213
COMPARE SIB

5.7 DISTRIBUTION

5.7.1 Definition

Distribute calls to different logical ends of the SIB based on user specified parameters.

5.7.2 Operation

This SIB distributes calls to its different logical ends based on a user identified algorithm. For example, calls could be distributed based on a percentage allocated to each logical end.

5.7.3 Potential service applications

- mass calling;
- televoting;
- freephone.

5.7.4 Input

5.7.4.1 Logical start

Indicates the logical start of execution for the SIB.

5.7.4.2 Service support data

- Algorithm type
 - percentage;
 - sequential;
 - time of day;
 - day of week.

NOTE 1 – Hierarchical call distribution may be realized through the use of multiple instances of the DISTRIBUTION SIB in conjunction with the STATUS NOTIFICATION SIB.

 - Number of logical ends

NOTE 2 – Unlike most SSD, change of this value will effect the structure of the GSL this SIB is contained in.

 - Algorithm parameters
 - If Type = percentage
 - For each logical end
 - percentage (sum over all paths must equal 100).
 - If Type = sequential
 - None
 - If Type = time of day
 - For each logical end
 - begin time associated with this logical end;
 - end time associated with this logical end.
 - All 24 hours of the day must be accounted for, with no overlap of time across logical ends.
 - If Type = day of week
 - For each logical end
 - all days of the week to be associated with this logical end.
 - All days of the week must be accounted for. No day may be associated with more than one logical end.
 - CIDFP-Error
 - This CID field pointer specifies where in output call instance data the error cause will be written.

5.7.4.3 Call instance data

- None

Recommendation Q.1213 (10/95) 13

14 Recommendation Q.1213 (10/95)

5.7.5 Output

5.7.5.1 Logical end

- 1
- 2
- ...
- N [where N = number of logical ends (item 1 of input SSD)]
- Error

5.7.5.2 Call instance data

- Error cause

Identifies the specific condition which caused an error during the operation of the SIB. The following errors have been identified for DISTRIBUTION:

- a) invalid type;
- b) invalid percentage allocation ($> 100, < 0$);
- c) invalid sum of percentage allocations (not equal to 100);
- d) invalid number of logical ends;
- e) missing time period;
- f) overlap of the time across logical ends;
- g) missing days;
- h) overlap of days across logical ends.

5.7.6 Graphical representation

See Figure 7.

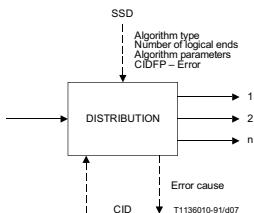


FIGURE 7/Q.1213
DISTRIBUTION SIB

5.8 LIMIT

5.8.1 Definition

Limit the number of calls related to IN provided service features. Such limiting will be based on user specified parameters.

NOTE – This SIB is not used for network congestion management functions.

Recommendation Q.1213 (10/95) 15

5.8.2 Operation

This SIB may be used to pass all or a fraction of all calls related to IN provided service features.

For example, calls may be passed:

- for a specific duration (which may be infinite) at specific intervals;
- according to a counting algorithm (e.g. pass N calls out of P).

The LIMIT SIB in conjunction with other SIBs (e.g. COMPARE) can provide the required functionality for time dependent call limiting (e.g. TOD).

5.8.3 Potential service applications

- mass calling;
- televoting;
- freephone.

5.8.4 Input

5.8.4.1 Logical start

Indicates the logical start of execution for the SIB.

5.8.4.2 Service support data

- Type
 - Specifies the type of limiting to be performed. The following types have been identified:
 - a) pass calls for (S) seconds out of every (Q) seconds;
 - b) pass (N) calls out of (P) calls.

Parameters

Specifies the parameters associated with the SSD type selected above:

- 1) S duration;
- 2) Q interval;
- 3) P counter interval;
- 4) N number of calls.

CIDFP-File

This CID field pointer specifies where the current limit count is located.

CIDFP-Error

This CID field pointer specifies where in output call instance data the error cause will be written.

5.8.4.3 Call instance data

- File
 - Identifies the data associated with CIDFP-File which specifies the current count of calls.

5.8.5 Output

5.8.5.1 Logical end

- pass;
- no pass;
- error.

16 Recommendation Q.1213 (10/95)

5.8.5.2 Call instance data

- Error cause

Identifies the specific condition which caused an error during the operation of the SIB. The following errors have been identified for LIMIT:

- a) invalid type;
- b) invalid parameter.

5.8.6 Graphical representation

See Figure 8.

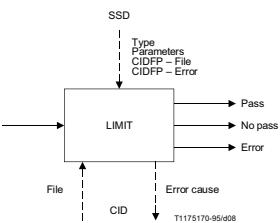


FIGURE 8/Q.1213
LIMIT SIB

5.9 LOG CALL INFORMATION

5.9.1 Definition

Log detailed information for each call into a file. The collected information may be used by management services (e.g. statistics, etc.) and not by call-related services.

5.9.2 Operation

This SIB logs (or writes) call related information to a specified file. The type of call-related information to be logged will be identified by service support data. Each instance of this SIB will cause the recording of the specified CID information.

5.9.3 Potential service applications

- All services.

5.9.4 Input

5.9.4.2 Service support data

CIDFP-Data

These CID field pointers specify which call instance data are to be used as identifiers. CIDFP-Data can include:

- a) call attempt time;
- b) call stop time;
- c) call connect time;
- d) dialled number;
- e) destination number;
- f) additional dialled number (e.g. credit card number, etc.);
- g) calling line identification;
- h) time in queue;
- i) bearer capability;
- j) error causes;
- k) any other CID.

Log file name

Specifies the log file object where the value of the identifier is to be logged.

CIDFP - Authorized Relationship Id

This CID field pointer specifies which call instance data is to be used as the Authorized Relationship Id.

CIDFP-Error

This CID field pointer specifies where in output call instance data the error cause will be written.

5.9.4.3 Call instance data

- Data
 - Specifies the data associated with the CIDFP-Data (see SSD) which is to be logged.
- Authorized Relationship Id
 - The Authorized Relationship Id provides the identity of the established Authorized Relationship through which the operations can be applied.

5.9.5 Output

5.9.5.1 Logical end

- Success (information written);
- Error.

5.9.5.2 Call instance data

- Error cause

Identifies the specific condition which caused an error during the operation of the SIB. The following errors have been identified for LOG CALL INFORMATION:

- invalid identifier;
- invalid log file indicator.

5.9.6 Graphical representation

See Figure 9.

Indicates the logical start of execution for the SIB.

Recommendation Q.1213 (10/95) 17

18 Recommendation Q.1213 (10/95)

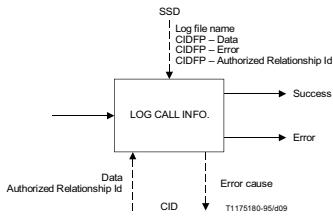


FIGURE 9/Q.1213
LOG CALL INFO SIB

5.10 QUEUE

5.10.1 Definition

Provide sequencing of IN calls to be completed to a called party.

5.10.2 Operation

This SIB provides all the processing needed to provide queueing for a call, and will specifically:

- pass the call if resources are available;
- queue the call;
- optionally play announcements to caller on queue;
- when resources become available, dequeue the call.

5.10.3 Potential service application

- All IN services which use call queueing service feature.

5.10.4 Input

5.10.4.1 Logical start

Indicates the logical start of execution for the SIB.

5.10.4.2 Service support data

- Max active
Specifies the maximum number of active calls allowed for the resource.
- Max number
Specifies the maximum number of calls allowed on queue at a given time.
- Max time
Specifies the maximum time the call may remain on the queue.

Recommendation Q.1213 (10/95) 19

- Announcement parameters
Specify the control values for announcements. The control values which can be specified are:
 - Announcement ID: specifies which announcement is to be sent; the Announcement ID could be "null" to signify that no announcement is to be sent.
 - Repetition requested: specifies if the announcement is to be repeated;
 - Repetition interval: specifies the delay period in seconds between repetitions;
 - Maximum repetitions: specifies the maximum number of times the announcement will be repeated.
- CIDFP-Call
This CID field pointer specifies which call instance data identifies the specific call.
- CIDFP-Resource
This CID field pointer specifies which call instance data identifies the resource.
- CIDFP-Error
This CID field pointer specifies where in output call instance data the error cause will be written.

5.10.4.3 Call instance data

- Call reference
Identifies the specific call which is a candidate for queueing.
- Resource
Specifies the data associated with the CIDFP-Resource which identifies the resource for which the call will be queued.

5.10.5 Output

5.10.5.1 Logical end

- 1) Resource available;
- 2) Call party abandon;
- 3) Queue timer expiry;
- 4) Queue full;
- 5) Error.

5.10.5.2 Call instance data

- Time spent in queue
Identifies the total time that a particular call was queued.
- Error cause
Identifies the specific condition which caused an error during the operation of the SIB. The following errors have been identified for QUEUE:
 - a) invalid Max active;
 - b) invalid Max number;
 - c) invalid Max time;
 - d) invalid announcement parameters;
 - e) invalid call reference.

5.10.6 Graphical representation

See Figures 10 and 11.

20 Recommendation Q.1213 (10/95)

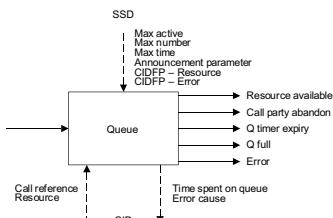


FIGURE 10/Q.1213
QUEUE SIB

5.11 SCREEN

5.11.1 Definition

Perform a comparison of an identifier against a list to determine whether the identifier has been found in the list.

5.11.2 Operation

This SIB takes the appropriate identifier and determines whether or not it is contained within the list identified by the SIB support data. A "Match" condition results if the identifier has been found on the list.

Examples using the SCREEN SIB are:

- for verifying a user ID or PIN;
- for terminating or originating call screening based on a network address.

Multiple instances of the SCREEN SIB, in conjunction with other SIBs, like TRANSLATE and COMPARE, may result in more complex screening capabilities.

5.11.3 Potential service applications

- Selective call forward on busy/don't answer;
- Originating call screening;
- Terminating call screening;
- Security screening;
- Account card calling;
- Credit card calling.

5.11.4 Input

5.11.4.1 Logical start

Indicates the logical start of execution for the SIB.

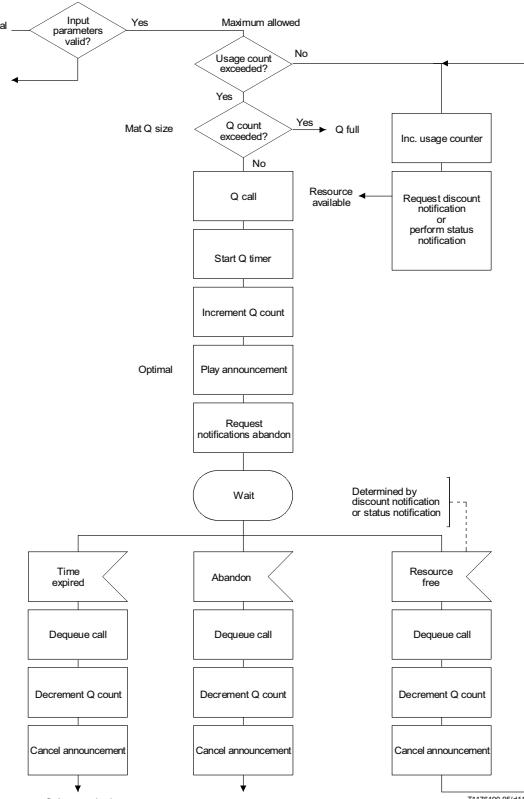


FIGURE 11/Q.1213
QUEUE SIB stage 1

Recommendation Q.1213 (10/95) 21

22 Recommendation Q.1213 (10/95)

5.11.4.2 Service support data

- Screen list name
The screen list name identifies the screen data object to be used.
- Screen list Filter
The Screen list Filter identifies the attributes and filter tests to be applied to the attributes in the screen data object. The attribute values are stored in the CIDFP – Screen pointers.
- CIDFP-Data
This CID field pointer(s) specifies which call instance data is to be used as the identifier(s).
- CIDFP – Authorized Relationship Id
This CID field pointer specifies which call instance data is to be used as the Authorized Relationship Id.
- CIDFP-Error
This CID field pointer specifies where in output call instance data the error cause will be written.

5.11.4.3 Call instance data

- Data
The Data CID is the attributes values associated with the CIDFP-Data (see SSD) which is to be filtered against the screen data object.
- Authorized Relationship Id
The Authorized Relationship Id provides the identity of the established Authorized Relationship through which the operations can be applied.

5.11.5 Output

5.11.5.1 Logical end

- Match [= on the list].
- CIDFP – Authorized Relationship Id
This CID field pointer specifies which call instance data is to be used as the Authorized Relationship Id.
- CIDFP-Error
This CID field pointer specifies where in output call instance data the error cause will be written.

5.11.5.2 Call instance data

- Error cause
Identifies the specific condition which caused an error during the operation of the SIB. The following errors have been identified for SCREEN:

 - invalid identifier;
 - invalid screen list.

5.11.6 Graphical representation

See Figure 12.

5.12 SERVICE DATA MANAGEMENT

5.12.1 Definition

Enables end user specific data to be replaced, retrieved, incremented, or decremented.

Recommendation Q.1213 (10/95) 23

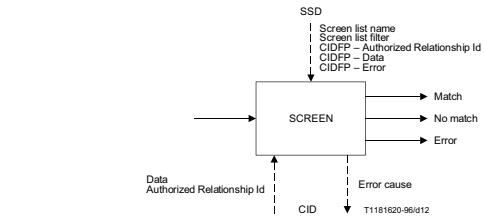


FIGURE 12/Q.1213

SCREEN SIB

5.12.2 Operation

This SIB performs the appropriate actions, i.e. replace, retrieve, increment, or decrement information stored within the network. For example, this SIB could be used to retrieve or replace a customer's call forwarding number.

5.12.3 Potential service application

- Call forwarding;
- Customer profile management.

5.12.4 Input

5.12.4.1 Logical start

Indicates the logical start of execution for the SIB.

5.12.4.2 Service support data

- Object name
Specifies the subscriber data object to be used.
- Action
Specifies the operation to be performed on the subscriber data. The following actions are allowed:
 - Replace – Replace the existing data element in the subscriber file specified by the element indicator with new data specified by the information value.
 - Retrieve – Copy the data element specified by the element indicator and place it in the output CID called data retrieved.
 - Increment – Increase the value of the data element in the subscriber file specified by the element indicator by the amount indicated by the Inc/Dec value.
 - Decrement – Decrease the value of the data element in the subscriber file specified by the element indicator by the amount indicated by the Inc/Dec value.

24 Recommendation Q.1213 (10/95)

- e) SetToDefault – Reset the value of the data attribute in the subscriber data object to its default value.
- f) addObject – Add a new data object into the database. In this case the Attribute indicator must contain all of the object attributes which are required to correctly initialize the data object.
- g) removeObject – Remove a data object from the database.

5.12.4.3 Call instance data

- Attribute indicator
Specifies the data attribute in the subscriber data object upon which the action is to be performed. This optional data parameter is only required when the field to be acted upon is constant for all call instances (e.g. changing a call forwarding number). A "null" in this SSD field indicates that the attribute indicator can vary and its value must be provided through call instance data.
- Inc/Dec value
Specifies the amount by which the attribute indicator is to be incremented or decremented.
- CIDFP-Info
This CID field pointer specifies which call instance data is to be used as the information value.
- CIDFP-Attribute
This CID field pointer specifies which call instance data is to be used as the attribute indicator. If the attribute indicator is to be specified by the SSD, then this CID field pointer will not be used by the SIB.
- CIDFP-Retrieve
This CID field pointer specifies where in call instance data the retrieved data element is to be written.
- CIDFP-Error
This CID field pointer specifies where in output call instance data the error cause will be written.

5.12.4.4 Call instance data

- Information value
Specifies the new value for the subscriber attribute data. This data is passed to this SIB from the user interaction SIB using the output CID parameter called collected data.
- Attribute indicator
- Authorized Relationship Id
The Authorized Relationship Id provides the identity of the established Authorized Relationship through which the operations can be applied.

5.12.5 Output

5.12.5.1 Logical end

- Success (record written or retrieved);
- Error.

5.12.5.2 Call instance data

- Retrieved Value(s)
Specifies the data attribute(s) values retrieved.

5.12.6 Error cause

Identifies the specific condition which caused an error during the operation of the SIB. The following errors have been identified for SERVICE DATA MANAGEMENT:

- a) invalid object indicator;
- b) invalid action;
- c) invalid attribute indicator;
- d) invalid information value;
- e) invalid Inc/Dec value.

5.12.6 Graphical representation

See Figure 13.

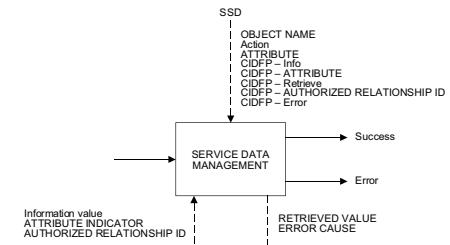


FIGURE 13/Q.1213

SERVICE DATA MANAGEMENT SIB

5.13 STATUS NOTIFICATION

5.13.1 Definition

Provide the capability of inquiring about the status and/or status changes of network resources.

5.13.2 Operation

There are four types of status notification requests:

- Poll resource status – Return the current status of the resource.
- Wait for status – Wait until the resource assumes the desired status unless the resource is already in the desired status.
- Initiate continuous monitor – Monitor and record the changes in busy/idle status; subsequent monitor – Return all the changes in status for the resource or other events as required.
- Cancel continuous monitor.

Recommendation Q.1213 (10/95) 25

26 Recommendation Q.1213 (10/95)

“Poll resource status” status notification could be used to determine if the destination address is busy or idle. In the busy case, “Wait for status” status notification could be used to notify service logic when the destination address becomes idle. “Initiate continuous monitor” status notification could be needed to create a resource history file.

5.13.3 Potential service applications

- CCBS;
- call distribution;
- freephone;
- call transfer.

5.13.4 Input

5.13.4.1 Logical start

Indicates the logical start of execution for the SIB.

5.13.4.2 Service support data

- Type
 - Specifies the type of operation for this SIB. Four types have been identified:
 - a) poll resource status;
 - b) wait for status;
 - c) initiate continuous monitor;
 - d) cancel continuous monitor.
- Resource
 - Specifies the particular entity to be monitored. The following resources can be monitored:
 - 1) lines;
 - 2) trunks.
- Timer
 - Specifies the maximum amount of time to monitor the resource. If the value of timer is “null” no time limit is specified. This SSD is not used if the type is set to “poll resource status” or “cancel continuous monitor”.
- Status notification file name
 - Specifies the file object where the current resource status is to be logged. If a “null” value is specified, the resource status will not be logged. This SSD is not used if type is set to “cancel continuous monitor”.
- Resource status
 - Specifies the desired status of the resource being monitored. This SSD is only used when the type is set to “wait for status”. Valid resource status’s are:
 - a) busy;
 - b) idle.
- CIDFP-Status
 - This CID field pointer specifies where in call instance data the resultant status of the resource is to be written.
- CIDFP-Error
 - This CID field pointer specifies where in output call instance data the error cause will be written.

Recommendation Q.1213 (10/95) 27

5.13.4.3 Call instance data

- None.

5.13.5 Output

5.13.5.1 Logical end

- Success
 - Poll resource status – Present status returned.
 - Wait for status – Line or resource has assumed the given status.
 - Initiate continuous monitor – Continuous monitor initiated.
 - Cancel continuous monitor – Continuous monitor terminated.
- Timer expiry (only used with “wait for status”).
- Error.

5.13.5.2 Call instance data

- Status
 - Specifies the current status of the resource.
- Error cause
 - Identifies the specific condition which caused an error during the operation of the SIB. The following errors have been identified for STATUS NOTIFICATION:
 - a) invalid type;
 - b) invalid resource;
 - c) invalid timer;
 - d) invalid file indicator;
 - e) invalid resource status.

5.13.6 Graphical representation

See Figure 14.

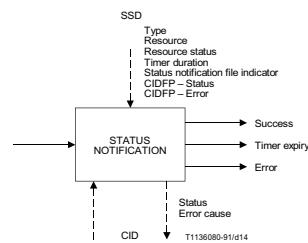


FIGURE 14/Q.1213

STATUS NOTIFICATION SIB

Recommendation Q.1213 (10/95)

5.14 TRANSLATE

5.14.1 Definition

Determines output information from input information.

5.14.2 Operation

This SIB translates input information and provides output information, based on the various other input parameters. Parameters provided identify which file should be scanned for the translation. Translation can be based on either input information only, or on input information and the CLI.

For example, this SIB could be used for modifying input information (for instance, dialled digits) into a standard numbering plan upon which network routing is based.

In conjunction with other SIBs, like COMPARE, the TRANSLATE SIB can provide the required functionality for time dependent routing.

5.14.3 Potential service applications

- Freephone;
- User-defined routing;
- VPN;
- UPT;
- Abbreviated dialling;
- Selective call forwarding on busy/don’t answer;
- Call forwarding;
- Call transfer.

5.14.4 Input

5.14.4.1 Logical start

Indicates the logical start of execution for the SIB.

5.14.4.2 Service support data

- Object Name
 - Specifies where the translation data object is located.
- Translate Filter
 - The Translate Filter identifies the attributes and filter tests to be applied to the attributes in the translate data object. The attribute values are stored in the CIDFP – Filter Value(s) pointers.
- Translated Attribute
 - Specifies which object attribute(s) is to be returned to Translated data value(s).
- CIDFP-Filter Value(s)
 - This CID field pointer(s) specifies which call instance data is to be used as the information.
- CIDFP-Translated Data
 - This CID field pointer specifies where in call instance data that the translated data attribute value is to be written.
- CIDFP - Authorized Relationship Id
 - This CID field pointer specifies which call instance data is to be used as the Authorized Relationship Id.

Recommendation Q.1213 (10/95) 29

- CIDFP-Error
 - This CID field pointer specifies where in output call instance data the error cause will be written.

5.14.4.3 Call instance data

- Filter Value(s)
 - Specifies the translate filter data value(s) to be used. Stored in CIDFP - Filter Value(s).
- Authorized Relationship Id
 - The Authorized Relationship Id provides the identity of the established Authorized Relationship through which the operations can be applied.

5.14.5 Output

5.14.5.1 Logical end

- Success;
- Error.

5.14.5.2 Call instance data

- Translated data
 - Specifies the data element(s) resulting from the translation.
- Error cause
 - Identifies the specific condition which caused an error during the operation of the SIB. The following errors have been identified for TRANSLATE:
 - a) invalid type;
 - b) invalid file indicator;
 - c) invalid information;
 - d) translation not available.

5.14.6 Graphical representation

See Figure 15.

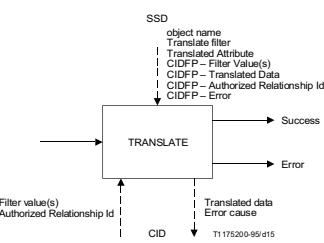


FIGURE 15/Q.1213

TRANSLATE SIB

Recommendation Q.1213 (10/95)

5.15 USER INTERACTION

5.15.1 Definition

Allows information to be exchanged between the network and a call party, where a call party can be either a calling or a called party.

5.15.2 Operation

This SIB provides a call party with information (e.g. announcements) and/or collects information from a call party.

The announcements can be, for example:

- DTMF tones;
- a customized or generic audio message;
- network progression tones (e.g. dial tone, busy tone, etc.).

The collected information can be, for example:

- DTMF tones;
- audio;
- IA5 string text.

This SIB provides the specified announcement (which may be null) to the user. Depending on the repetition type (i.e. count, time), the message is repeated until the repetition number or time is reached.

Expected user input may be null. Assuming it is not null and user interruptibility is allowed, the message is stopped upon initial input by the user. If user interruptibility is not allowed or the message (or message sequence) is completed with no input from the user, the first input should be received within the initial response time after the message (or message sequence) is terminated, otherwise an error condition results.

User input is considered complete when the maximum number of characters has been reached, or an end delimiter character is received, or the inter-digit timer has been exceeded.

The stage 2 SDL representation of this SIB may be helpful in understanding its operation. Refer to 5.2.12/Q.1214.

5.15.3 Potential service applications

- Most IN CS-1 services will require user interaction.

5.15.4 Input

5.15.4.1 Logical start

Indicates the logical start of execution for the SIB.

5.15.4.2 Service support data

- Announcement parameters
 - Specify the following control values for announcements:
 - a) Announcement ID
 - Specifies which announcement is to be sent. The Announcement ID could be "null" to signify that no announcement is to be sent.
 - b) Repetition requested
 - Specifies if the announcement is to be repeated.
 - c) Repetition interval
 - Specifies the delay period in seconds between repetitions.
 - d) Maximum repetitions
 - Specifies the maximum number of times the announcement will be repeated.

Recommendation Q.1213 (10/95) 31

e) Duration

Specifies the maximum length of time the announcement will be played.

– Collect information parameters

Specify the control values for user entered information.

1) User interruptibility

Specifies if an announcement can be interrupted by the call party entering information (yes or no).

2) Voice feedback

Specifies if the user is given a vocalization of the users input.

3) Type

Specifies the expected form of the user entered information. The following forms can be identified:

i) DTMF;

ii) audio;

iii) IA5 string;

iv) null (where null signifies that no data is to be collected).

4) Maximum number of characters

Specifies the maximum number of characters to collect, (> 0 , where 0 identifies non-character input).

5) Minimum number of characters

Specifies the minimum number of characters to collect, (\leq the maximum, ≥ 0 , where 0 identifies non-character input).

6) Initial input waiting timer

Specifies the maximum time to wait for beginning of call party's response.

7) Inter-character waiting timer

Specifies the maximum time to wait after a pause by the call party.

8) End delimiter

Specifies special character(s) signifying the end of an input. If this parameter is "null", no delimiter is specified.

– CIDFP-Call_Party

This CID field pointer specifies which call instance data is to be used to identify the call party.

– CIDFP-Collected

This CID field pointer specifies where in output call instance data that the call party entered data is to be written.

– CIDFP-Error

This CID field pointer specifies where in output call instance data the error cause will be written.

5.15.4.3 Call instance data

– Call party identifier

Specifies the data associated with the CIDFP-Call_Party which identifies the call party exchanging information with the network.

32 Recommendation Q.1213 (10/95)

5.15.5 Output

5.15.5.1 Logical end

- Success;
- error.

5.15.5.2 Call instance data

- Collected data
 - Specifies the data collected by the network from the call party.
- Error cause
 - Identifies the specific condition which caused an error during the operation of the SIB. The following errors have been identified for USER INTERACTION:
 - a) call abandon;
 - b) collection time out (no input received);
 - c) incorrect number of digits received;
 - d) announcement resource unavailable;
 - e) data collection resource unavailable;
 - f) invalid announcement ID;
 - g) invalid call party;
 - h) inconsistent timer setting;
 - i) call status incompatible with playing of announcements;
 - j) call status incompatible with collecting information.

5.15.6 Graphical representation

See Figure 16.

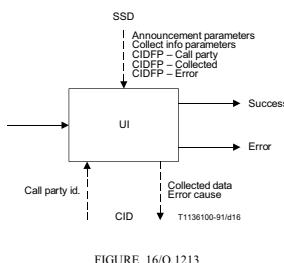


FIGURE 16/Q.1213
USER INTERACTION SIB

5.16 Operation

Information is compared with the format expected for the data. The VERIFY SIB normally follows the USER INTERACTION SIB when information has been collected from a call party.

The service support data identifies the type of data format. This SIB compares the input data to that expected format.

This SIB may, for example, be used when there is a need to verify the syntax of information. This could be:

- a user identification;
- a network address;
- any extra dialogue such as PIN code dialling or answer to a call prompt.

5.16.3 Potential service applications

- Freephone;
- selective call forwarding;
- UPT;
- televoting.

5.16.4 Input

5.16.4.1 Logical start

Indicates the logical start of execution for the SIB.

5.16.4.2 Service support data

- Maximum number of characters
 - Specifies the maximum number of characters allowed.
- Minimum number of characters
 - Specifies the minimum number of characters allowed.
- Format
 - Format specifies the expected syntax of the data being verified. The format is specified using "code" characters. The following "codes" have been identified:
 - 1) x Any character;
 - 2) L Any letter;
 - 3) A Upper case letters only;
 - 4) a Lower case letters only;
 - 5) D Any digit (0-9) or delimiter (#, *);
 - 6) N Any digit (0-9);
 - 7) n Any digit except 0 (1-9);
 - 8) [x] Optional character, where x represents any of the specified "codes";
 - 9) \x\ Specific character(s) required (e.g. \01) indicated that either a 0 or a 1 must be present at that designated position in the data being verified).
 - For example, the format "NNNN\c" would indicate that a PIN code of 2387c would pass syntax verification, while 2387d would fail.
- CIDFP-Data
 - This CID field pointer specifies which call instance data is to be used as the identifier to be verified.
- CIDFP-Error
 - This CID field pointer specifies where in output call instance data the error cause will be written.

5.16 VERIFY

5.16.1 Definition

Provide confirmation that information received is syntactically consistent with the expected form of such information.

Recommendation Q.1213 (10/95) 33

34 Recommendation Q.1213 (10/95)

5.16.4.3 Call instance data

- Data

Specifies the data associated with the CIDFP-Data which is to be verified.

5.16.5 Output

5.16.5.1 Logical end

- Pass;
- Fail;
- Error.

5.16.5.2 Call instance data

- Error cause

Identifies the specific condition which caused an error during the operation of the SIB. The following errors have been identified for VERIFY:

- invalid format;
- invalid identifier;
- inconsistent Max/Min number of characters specified.

5.16.6 Graphical representation

See Figure 17.

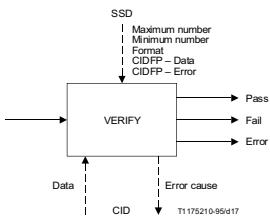


FIGURE 17/Q.1213
VERIFY SIB

6 Basic call process

6.1 General

The Basic Call Process (BCP) has been defined in 4.0/I.329/Q.1203 [2] as a specialized SIB which provides the basic call capabilities.

These capabilities enable the use of GSL as well as other SIBs to completely describe IN CS-1 services and service features.

Recommendation Q.1213 (10/95) 35

Continue with existing data

This POR identifies that the BCP should continue call processing with no modification.

Proceed with new data

This POR identifies that the BCP should proceed with call processing with only a data modification.

Handle as transit

This POR identifies that the BCP should treat the call as if it had just arrived.

Clear call

This POR identifies that the BCP should clear the call.

Enable call party handling

This POR identifies that the BCP should perform functions to enable call control for individual call parties.

The use of this POR and the definition of any additional SIBs needed to support call party handling, are for further study.

Initiate call

This POR identifies that the call should be initiated. This may be independent of an existing call, or may be in the context of an existing call.

6.3 BCP stage 1 description

6.3.1 Definition

This specialized SIB allows access to IN services/service features represented through the use of chains of SIBs and global service logic. The interface points between this SIB and GSL are described as POIs and PORs.

6.3.2 Operation

The BCP contains a set of armed POIs, and if during the processing of a call, one of these POIs is encountered, a chain of SIB is executed through global service logic.

When the chain of SIB terminates, call processing may be influenced according to the specified POR.

NOTE – Non-IN supported services are processed in the BCP and no GSL processing is required.

6.3.3 Potential service applications

- All IN CS-1 services.

6.3.4 Output

Specifies the POI and data parameters which are passed to GSL.

6.3.4.1 Logical output

Initiate global service logic from a specified POI.

6.3.4.2 Service support data

- Set of POIs
- Specifies the points in the BCP where IN service logic processing can occur for a given service.
- CIDFP-CLI

This CID field pointer specifies which call instance data is to be used as the CLI.

It is not necessary or intended to fully model the BCP on the GFP in IN CS-1, but rather to insure that the functionality of the BCP that is required on the GFP in conjunction with SIBs be available to fully support IN CS-1 services/service features.

6.2 Points of initiation and points of return

The BCP functional interfaces to the global service logic in the GFP are described as Points of Initiation (POI) and Points of Return (POR). These are defined in 4.2/I.329/Q.1203.

IN CS-1 service flexibility is provided by defining specific POI and POR interfaces between the BCP and GSL. This flexibility allows a chain of SIBs to represent different services based on the launching POI and the returning POR.

For example, a SIB chain which screens a network address against a list could represent an originating call screening service if the address analysed POI launches the chain. However, if the prepared to complete call POI was used to launch the same chain, a terminating call screening service could result.

Furthermore, using the screening example from above, different services can result based upon which POR is used to complete the chain. If a "Match" logic end of the SCREEN SIB, is followed by a proceed with new data POR, a call is allowed to complete and this is an example of positive screening. However, negative screening, or call blocking, can be done with the same SIB chain by having the "Match" followed by a clear call POR.

6.2.1 List of POIs

The following set of POIs has been identified for IN CS-1.

Call originated

This POI identifies that the user has made a service request without yet specifying a destination address (e.g. off-hook but before dialling).

Address collected

This POI identifies that the address input has been received from the user.

Address analysed

This POI identifies that the address input has been analysed to determine characteristics of the address (e.g. freephone number).

Prepared to complete call

This POI identifies that the network is prepared to attempt completion of the call to the terminating party.

Busy

This POI identifies that the call is destined for a user who is currently busy.

No answer

This POI identifies that the call has been offered to a user who has not answered.

Call acceptance

This POI identifies that the call is active but the connection between the calling and called parties is not established (e.g. called party off-hook but no switch-through).

Active state

This POI identifies that the call is active and the connection between the calling and called parties is established.

End of call

This POI identifies that a call party has disconnected.

6.2.2 List of PORs

The following set of PORs has been identified for IN CS-1.

36 Recommendation Q.1213 (10/95)



Instituto Universitário de Lisboa
Lisbon University Institute

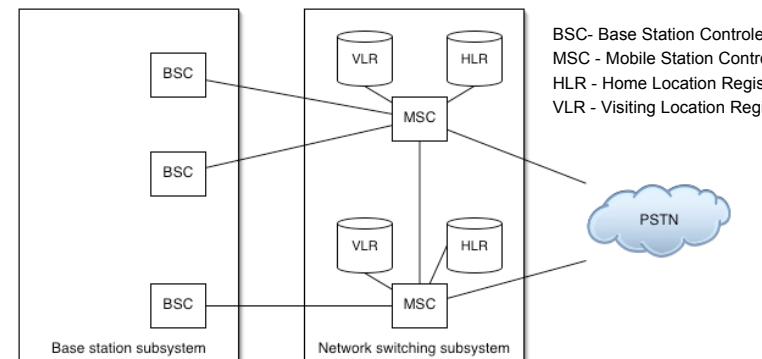
**Rede Inteligente
e as redes móveis
e a Internet**

Definições de mobilidade, desafios

- Mobilidade terminal
 - Um terminal móvel pode-se ligar via rádio a diferentes estações base, transferir a ligação rádio durante chamada (*handover*), ou a diferentes operadores (*roaming*)
- Mobilidade pessoal
 - O utilizador pode mudar de terminal e registar-se para efectuar ou receber chamadas em diferentes terminais (parcialmente suportado pelos SIM)
- Mobilidade dos serviços
 - O utilizador continua a ter acesso ao mesmo conjunto de serviços (aplicações e conteúdos) em qualquer rede em que se encontre
- Desafios para a arquitectura da IN
 - Resultante da mobilidade: que SCF deve ser utilizado ?
 - Segurança: como autenticar utilizadores, terminais, e elementos da rede?

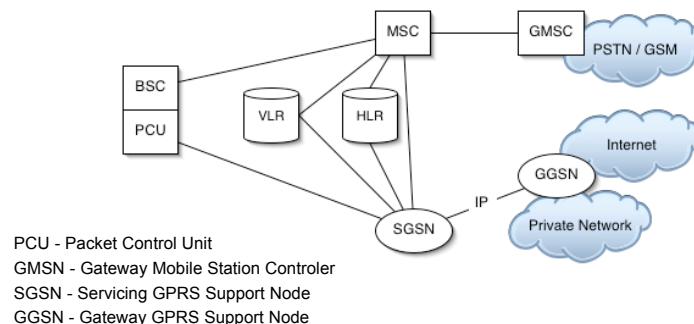
A arquitectura do sistema GSM

- O elemento obvio para a interacção com a rede móvel é o MSC (muito semelhante ao CCF/SSF da IN)
- Mas à que contar com a questão da mobilidade

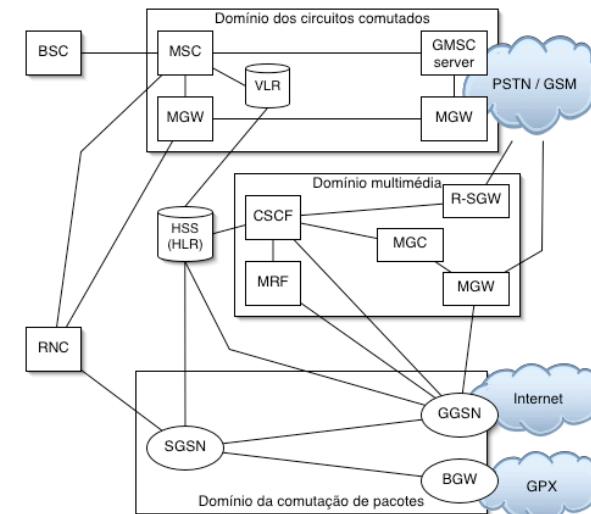


A arquitectura do sistema GPRS

- Bastante semelhante à do GSM:
 - introdução do conceito de *Gateway*
 - Introdução de elementos relacionados com a comutação de pacotes



A arquitectura do sistema UMTS

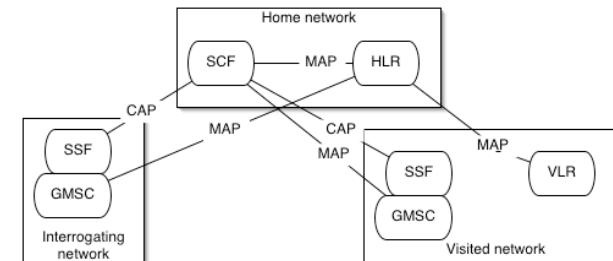


CAMEL

- **Customized Application of Mobile Enhanced Logic**
 - Iniciativa do ETSI para introduzir os conceitos da IN no GSM e garantir a interoperabilidade entre ambos
- Resultado da desadequação do CS-1, CS-2 e CS-3 à rede GSM
- Diferentes fases:
 - Fase 1 (1996): Baseada no CS-1 (*Anytime interrogation*)
 - Fase 2 (1997): Extensão ao modelo de chamada (acções fora do contexto de uma chamada), interacção com o SRF e com os serviços suplementares do GSM
 - Fase 3 (1999): suporte para o GPRS, disparo devido a eventos SMS e mobilidade

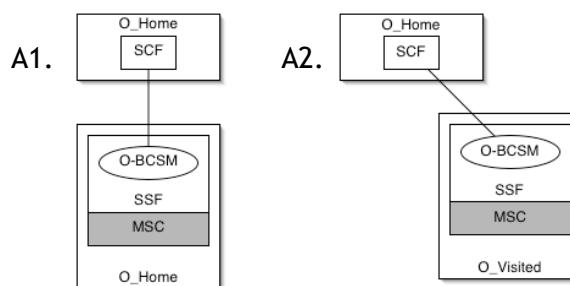
Arquitectura CAMEL

- Distinção entre: rede origem (*home*), visitada (*visited*) e interrogadora (*interrogating*)
 - O CAMEL apresenta uma versão simplificada do BCSM (ex., não há Mid_Call)
 - Definidos dois protocolos:
 - CAP: CAMEL Application Part (variantes do INAP para o GSM): usado para a interacção entre o SSF (associado a MSC) e o SCF
 - MAP: Mobile Application Part: usado para a interacção entre o SCF e o HLR (através de ATI - *anytime interrogation*)
- Ambos usam o SS7 da mesma forma que o INAP



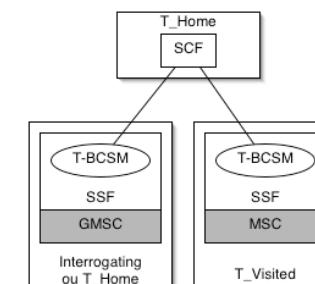
Execução e depoletar de serviços (0)

- Serviços são sempre executados no SCF da rede origem (*home network*) do terminal a que está associado o serviço, mas pode ser despoletado (*triggered*) por diferentes redes dependendo se o serviço é originado ou terminado; e de onde se encontra o terminal ao qual está associado o evento na sua rede origem (*home network*) ou noutra rede (*visiting network*)
 - A. Chamada originada (*outgoing*): o evento é disparado
 1. no O_BCSM por acção do MSC da *home network*
 2. ou do MSC da rede visitada em caso de *roaming*.



Execução e depoletar de serviços (T)

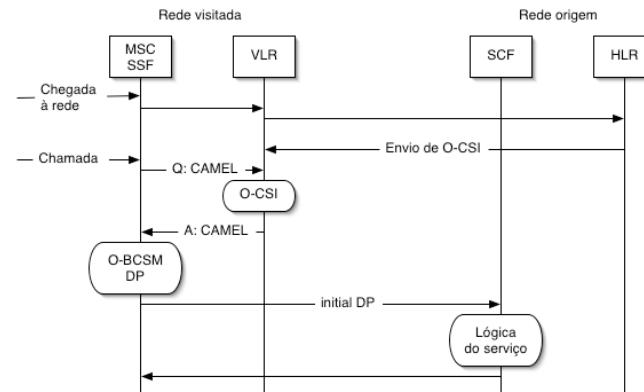
- Serviços são sempre executados no SCF da rede origem (*home network*) do terminal a que está associado o serviço, neste caso o chamado (*terminating*).
- (Para evitar o efeito de trombone (*tromboning*) as redes GSM fazem um encaminhamento directo não sendo contactada a *home network*. Isto obriga à definição de conceito de *interrogating network*. A *interrogating network* pode ser a *home network* do terminal chamado ou outra qualquer.)
 - B Chamada recebida (*incoming/terminating*): o GMSC da *interrogating network* contacta o HLR na *home network* do chamado por forma a verificar se existem DPs armados. Caso existam o seu SSF deverá quando adequado contactar o MSC da *home network*. No caso em que o chamado se encontre numa *visited network* esta deverá ainda receber informação sobre que DPs estão activados.



Armar DPs em redes visitadas

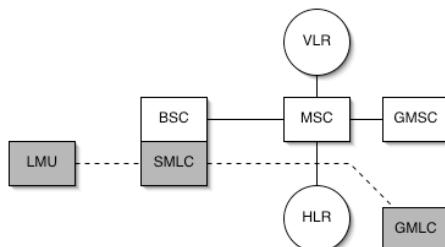
- O CAMEL usa o CAMEL subscription information (CSI) para armar DPs nas redes visitadas (ou interrogadoras), envio do CSI pelo HLR

Tipo de informação de subscrição	Armazenada no
CSI de chamada originada (outgoing) O-CSI	VLR da rede visitada
CSI de chamada recebida (terminating) T-CSI	GMSC da rede interrogadora
CSI de chamada recebida em rede visitada VT-CSI	VLR da rede visitada



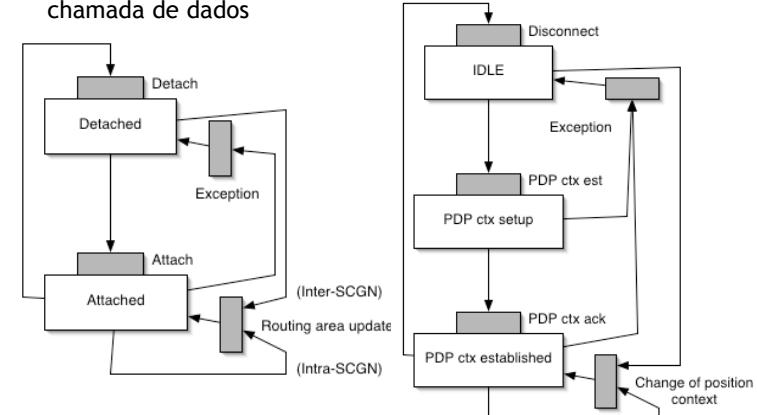
CAMEL: alguns exemplos (Location)

- Serviço de localização
 - Maior precisão que a célula em que o terminal se encontra
 - Elementos da rede envolvidos no serviço
 - *LMU - Location Measurement Unit*
 - *SMLC - Servicing Mobile Location Center*
 - *GMLC - Gateway Mobile Location Center*



CAMEL fase 3: suporte para o GPRS

- Definição de dois modelos de estados de chamada
 - *Attach-detach*: Suporte para a mobilidade no contexto do GPRS
 - Semelhante ao BCUSM do CS-2 da IN
 - *PDP context*: Suporte para o estabelecimento de contextos num chamada de dados



Mobilidade das aplicações

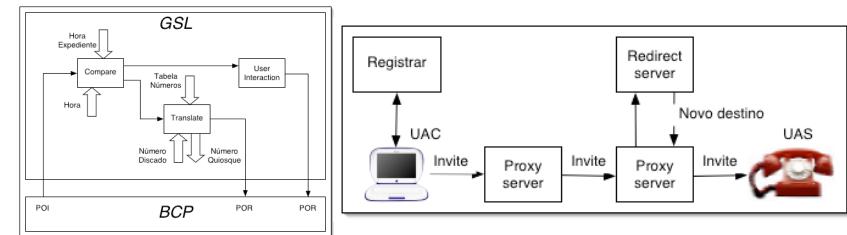
- Diferentes formas de suporte à mobilidade das aplicações
 - MExE: Mobile Execution Environment - ETSI
 - Plataforma para execução de código no terminal
 - Normalização de níveis de funcionalidade suportados pelos terminais (classmarks)
 - 1. WAP: Suporte para WML e WMLScript
 - 2. Java 2 Standard Edition (J2EE): JavaApplets e JavaPhone
 - 3. Java 2 Micro Edition (J2ME): Ambientes de execução com restrições. interfaces para a configuração da ligações com capacidade limitada e para o perfil do terminal
 - Diferentes cenários de utilização do MExE
 - Thin client mode, Applet Model, Peer-to-peer model
 - SIM application toolkit - ETSI
 - Lógica da aplicação e ambiente de execução no cartão SIM
 - Virtual Home Environment - VHE -3GPP
 - Portabilidade do perfil do utilizador (incluindo serviços) através das diferentes redes que visita

Serviços conferência multimédia sobre IP

- Exemplos: Voz sobre IP (VoIP), Telefonia sobre IP (IPtelephony)
- Problema fundamental
 - Serviços que têm requisitos de temporização fortes, atrasos $O(100ms)$
 - Rede - por comutação de pacotes (*store and forward*) - que não possui mecanismos (pelo menos disponíveis universalmente) de garantia de QoS determinística.
- Algumas soluções:
 - IETF:
 - Megaco (*Media Gateway Controller*) / H.348
 - Baseadas em SIP (*Session Initiation Protocol*) e RTP, RTCP
 - ITU-T: Norma H.323 "ITU-T Recommendation H.323: Packet-based multimedia communications systems"
 - Objectivo: Definição de uma tecnologia para comunicações multimédia (áudio, voz, texto, dados) através de redes por pacotes. Estas comunicações podem ser ponto-a-ponto ou multiponto, com participantes cujo acesso é feito através de diferentes redes (Internet, RDIS, Rede telefónica pública comutada).

Redes Inteligentes e o SIP

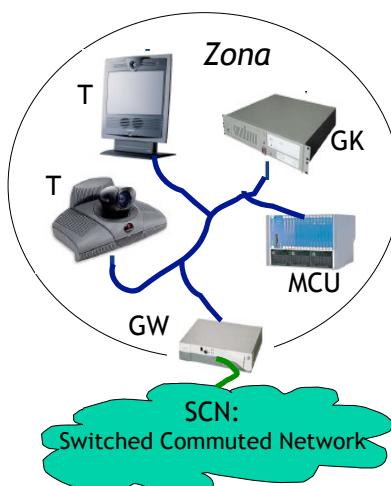
- Algumas diferenças entre a IN e o SIP
 - Modelo de processamento diferente na IN (controlo/notificação) e no SIP (transferência)



Elementos da arquitetura do SIP

- *User Agent Clients (UAC)* e *User Agent Servers (UAS)* - origem e terminação da chamada
- *Proxy Servers* - processa e transfere pedidos SIP as acções realizadas dependem da aplicação SIP a correr no proxy (e.g., localização, bloqueio de chamadas)
- *Redirect Servers* - tradução de endereços no pedido SIP
- *Registrar* - registo de terminais

Arquitectura lógica H.323 (simples)



T: Terminal

Equipamento dos utilizadores finais

GK: Gatekeeper

RAS: Registration, Admission e Status
Ex. Taxação, gestão da argura de banda

MCU: Multipoint Control Units

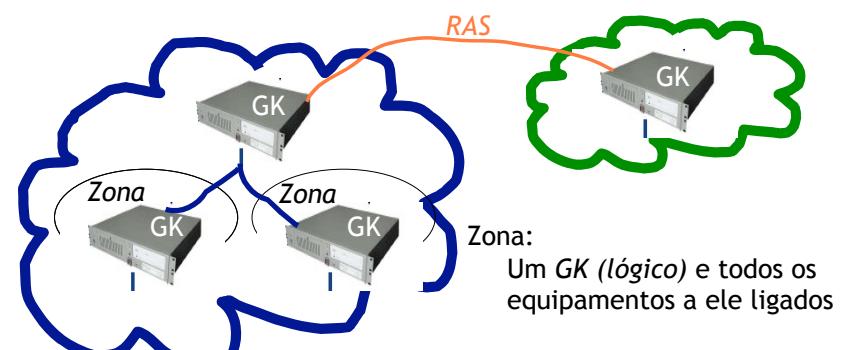
Gestão de comunicações multiponto
Composto por *Multipoint Controller* e *Multipoint Processors* (opcional)

GW: Gateway

Responsável pela tradução de protocolos e troca de dados entre rede H.323 e não-H.323
Composto por:

MGC: *Media Gateway Controller*
MG: *Media Gateway*

H.323 domínio administrativo

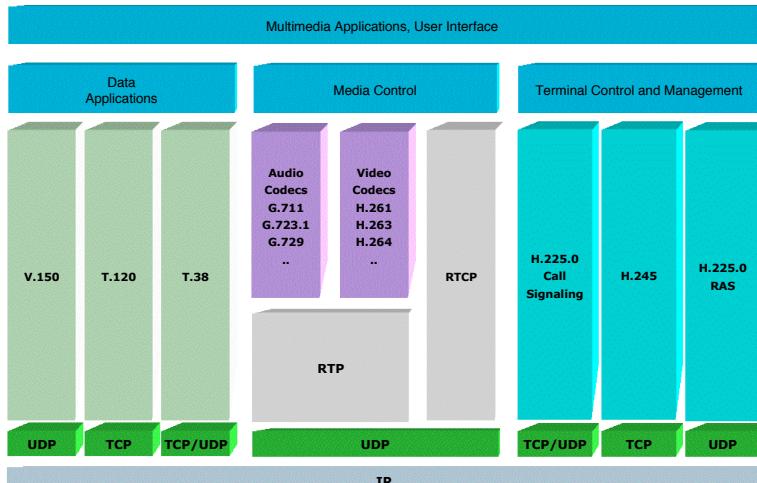


Zona:
Um GK (lógico) e todos os equipamentos a ele ligados

Domínio administrativo:

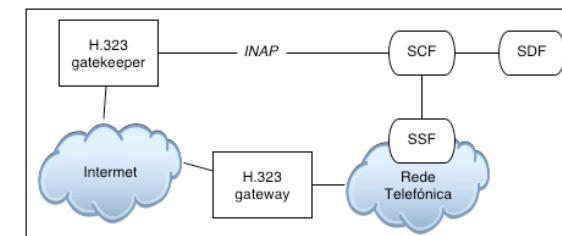
Conjunto de zonas sob um mesmo controlo administrativo

Arquitectura protocolar H.323



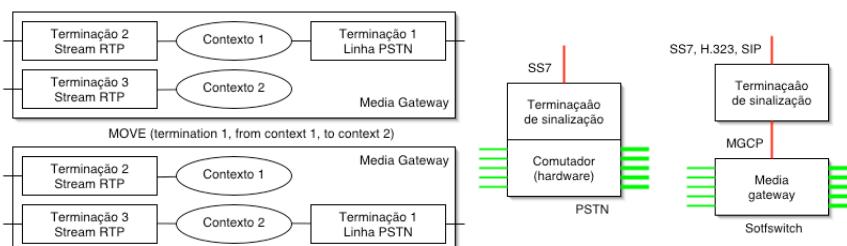
Redes Inteligentes e a H.323

- Semelhanças entre as funcionalidades executadas no *gatekeeper* H.323 e no SCF:
 - Admissão de chamadas / utilizadores
 - Autorização de chamadas
 - Bloqueio de chamadas (*screening*)
 - Auditoria e taxação
 - Gestão de chamadas
 - Monitorização das chamadas em actividade, em estabelecimento.
 - Re-encaminhamento de chamadas (ex., no caso de chamado ocupado)
 - Tradução de endereços:
 - Tradução de números de telefone em endereços IP (e vice-versa)
- Integração entre a IN e a H.323
 - Execução e lógica dos serviços (entre o SCF e o *gatekeeper*)
 - Fluxos de media (através do *gateway*)



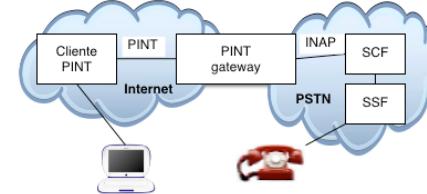
MGCP e Softswitching

- Separação entre o *media gateway controller* e o *media gateway*
- *Media Gateway Control Protocol* - MGCP, definido pela H.323 como o intermediário entre diferentes redes (ex. Internet e PSTN)
- Elementos fundamentais do MGCP: terminações e contextos
 - *Terminação*: ponto no *media gateway* que envia (*source*) ou recebe (*sink*) fluxos de media, pode ser físico (terminação telefónica) ou virtual (*stream RTP*)
 - *Contexto*: descreve os fluxos de media entre as terminações no *media gateway*
 - Semelhanças com o CSV do *Capability Set* 2
- Comandos MGCP: controlam terminações e contextos



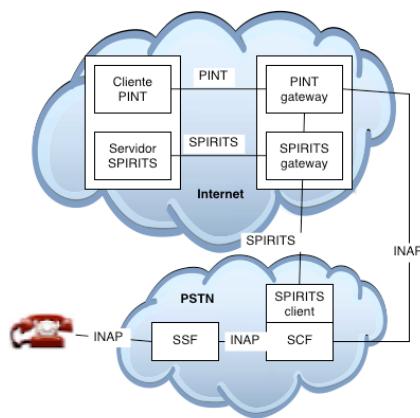
Interacção entre a Internet e a IN: PINT

- *Public Switched Telephony Network Internet Internetworking* - PINT
 - RFC 2848 - *The PINT Service Protocol: Extensions to SIP and SDP for IP Access to Telephone Call Services*
- Protocolo (não é um serviço) definido pelo IETF baseado no SIP (extende-o)
 - Introdução de números de telefone nos endereços
 - Novas mensagens (para notificações do estado da chamada): *subscribe*, *unsubscribe*, *notify*
 - As mensagens PINT podem conter a própria media (ex. o texto para um fax, um URL)
- Definição de alguns cenários:
 - *Click to dial, click to fax*: pedido, a partir da Internet, para o estabelecimento de uma chamada (envio de um fax)
 - *Click to fax-back*: pedido, a partir da Internet, para que nos enviem um fax
 - *Voice access to content*: pedido, a partir da Internet, para acesso a conteúdo
- Arquitectura (típica, não obrigatória)
 - *PINT client*: programa computacional com acesso a Internet (ex. Java servlet)
 - *PINT gateway*: intermediário entre a Internet e a IN: tradução para INAP



Interacção entre a IN e a Internet: SPIRITS

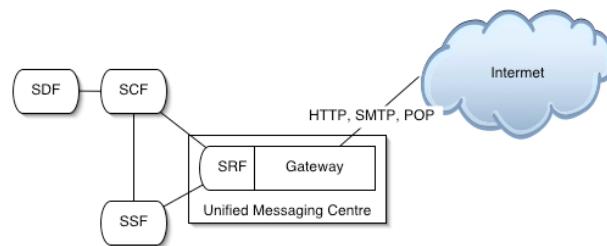
- Services in PSTN requesting Internet Services - SPIRITS
 - RFC 3136 - The SPIRITS Architecture
 - RFC 3910 - The SPIRITS (Services in PSTN requesting Internet Services) Protocol
- Motivado pela funcionalidade: Internet call waiting - ICW
 - Outros serviços exemplo: Internet Caller ID Delivery, Internet Call Forwarding
- Arquitectura



- Cliente/gateway PINT
 - Utilizada para o registo com o SCF por forma a activar o serviço (baseado em SPIRITS)
- Servidor SPIRITS
 - Recebe os eventos vindos do SCF, eventualmente possui a lógica de como tratar a chamada que chega (ex., Internet Call Forwarding)
- Cliente SPIRITS
 - Recebe os eventos do SCF (ex., chamada para o utilizador) e envia-os para o servidor
- Gateway SPIRITS
 - Necessário para filtrar eventos e/ou implementar alguma lógica de serviço

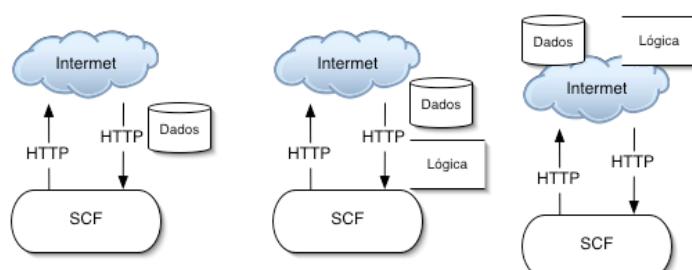
Unified messaging - UM

- Recepção de diferentes mensagens (voz, fax, email, SMS, MMS) numa mesma "caixa de correio"
- Algumas funcionalidades necessárias
 - Voice-to-email, Email-to-voice, Fax-to-email, etc
- Arquitectura
 - O componente central é o UMC: SRF e gateway com a Internet



Inteligência e gestão via Web: Web-IN

- Ideia inicial da Web-IN
 - Customização dos serviços (alteração dos dados do serviço) através da Web
 - Antes da Web-IN apenas possível através dos serviços de gestão (SMF) e com a cooperação do fornecedor de serviço
- Opções mais radicais
 - O SCF obtém da Internet não só os dados do serviço mas também a sua lógica
 - Os dados e a lógica do serviço estão na Internet e a sua execução é também externa ao SCF



“Inteligência” na Internet

- A “inteligência” na Internet é conhecida como activação ou programabilidade da rede
- Motivações:
 - A necessidade da introdução de novos serviços
 - de forma rápida, segura e económica
 - necessidade dos serviços serem implementados no
 - Ex., um novo algoritmo de selecção/eliminação de pacotes, multicast
 - sem estar dependente:
 - Organismos de normalização (processo lento)
 - Fabricantes: arquitecturas pouco flexíveis dos routers (substituição cara)
- Duas visões: programabilidade e activação
- Programabilidade:
 - Abertura das interfaces dos elementos da rede (ex., routers) à programação por terceiros
 - Visão típica dos operadores de telecomunicações
 - Iniciativas relevantes: IEEE P1520 e Xbind
- Activação:
 - Pacotes (cápsulas) na rede transportam o código a ser executado nos nós da rede
 - Visão típica da Internet
 - Iniciativas relevantes: PLAN e ANTS

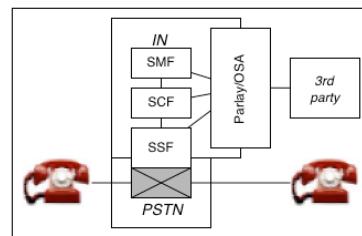


Instituto Universitário de Lisboa
Lisbon University Institute

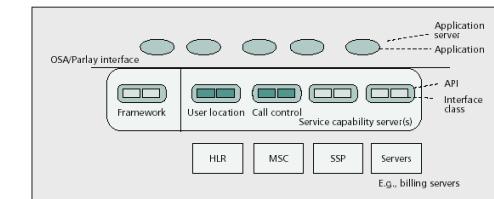
Parlay / OSA

Abertura dos serviços: Parlay/OSA

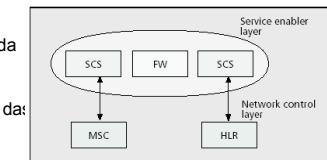
- **Ideia chave:** abrir o desenvolvimento de aplicações de telecomunicações
 - As outras entidades que não os operadores ou fabricantes (*3rd party*)
 - Definição de APIs normalizadas para o acesso a rede e criação de serviços
 - a um maior leque de pessoas...
 - Desenvolvimento de aplicações sem o conhecimento aprofundado de telecomunicações (abstracção dos protocolos e tecnologias de telecomunicações)
- Parlay/OSA criado pelo Parlay Group: 3GPP e ETSI
 - Aplicação: Serviço usado pelo utilizador final (*end-user*)
 - API: Interface, em termos de IN corresponde ao acesso ao SCF
 - Segurança é um aspecto fundamental (acesso total vs. apenas notificações)



Entidades lógicas Parlay/OSA

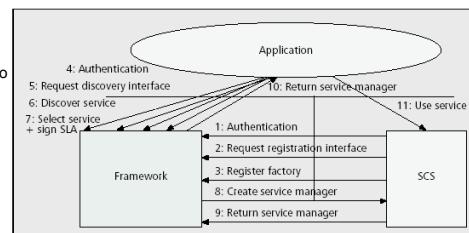


- SCS implementam a parte servidor e as Aplicações a parte cliente das APIs
- SCS interagem com os elementos chave da rede (e.g., SSP, HLR)
- A Framework controla e medeia o acesso das aplicações aos serviços
- OSA acrescenta ao Parlay recomendações para o mapeamento das interfaces nos protocolos de acesso à rede



A API Framework

- Inspirado na arquitetura TINA
- Acesso controlado as APIs
 - Autenticação e segurança
 - Descoberta de aplicações
- Inclusão de múltiplos vendedores e APIs adicionais não normalizadas
- Núcleo central de interfaces:
 - *Trust and security management*: autenticação de domínios
 - *Registration*: registo de novos SCSs
 - *Service life cycle management* e *Service discovery*: criação de novas API e descoberta de API
 - *Contract management*: gestão de contratos entre os diferentes participantes
- 1-3: Registo do SCS com a Framework
- 4: Autenticação do domínio da aplicação e verificação do contrato de serviço
- 5-6: Descoberta do serviço
- 7: Estabelecimento do contrato do tipo SLA
- 8-9: Criação de uma instância do serviço
- 10-11: Utilização do serviço



As aplicações Parlay/OSA

- Servidores de aplicações
 - Suporte para a abstração da distribuição (ex., CORBA)
 - Mapeamento das interfaces no protocolo de acesso aos elementos da rede (normalizado no caso do OSA)
 - Suporte para API em linguagens de programação comuns (ex., JAIN, JavaBeans)
 - Disponibilização de SDK (ex., Parlay/OSA SDK da Ericsson)

As interfaces Parlay/OSA

API	Descrição
Framework	Segurança, integridade, autenticação
Call Control	Estabelecimento, fecho e gestão de chamadas, conferências e chamadas multimédia. Notificações associadas a chamadas ou ligações. Diferentes especializações (Generic Call Control, Multiparty Call Control)
Data Session Control	Estabelecimento, fecho e gestão de sessões de dados (ex., transferência de ficheiros)
User Interaction	Interacção com o <i>end-user</i> para tocar ou apresentar mensagens e/ou recolher informação introduzida pelo <i>end-user</i>
Mobility	Obtenção de informação sobre a localização e/ou estado do <i>end-user</i>
Generic Messaging	Envio e recepção de mensagens (email, voz, SMS, MMS). Gestão de caixas de correio, voz
Terminal Capabilities	Obtenção de informação sobre as capacidades de um terminal (ex., tipo e resolução do ecrã)
Connnectivity Management	Negociação e gestão da qualidade de serviço (QoS) e contratos de nível de serviço (SLA) em redes IP
Acccount Mgmt.	Criação, remoção e gestão de contas de assinantes
Charging	Reserva ou cobrança de fundos de acordo com a conta de um assinante

As interfaces Parlay/OSA

- Especificadas e descritas utilizando a orientação aos objectos
 - Normativo
 - Especificação de interfaces (IDL) e definições de tipos de dados (IDL)
 - Informativo
 - Diagramas de classes (UML) e diagramas de sequências de estados (UML)
- Estrutura genérica de uma interface
 - Implementação da interface em duas partes (rede e aplicação)
 - Do lado da rede
 - Ip<Interface>* operações para controlar os recursos da rede
 - Ip<Interface>Manager* criação e gestão de instâncias de *Ip<Interface>*. Pedidos de notificações de eventos no servidor da aplicação
 - Do lado da aplicação (analogia *callback* interfaces)
 - IpApp<Interface>* recepção resultados e notificações da parte rede da interface
 - IpApp<Interface>Manager* criação/gestão de instâncias de *IpApp<Interface>*

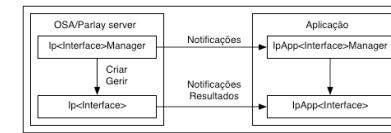


Diagrama de classes da interface CallControl

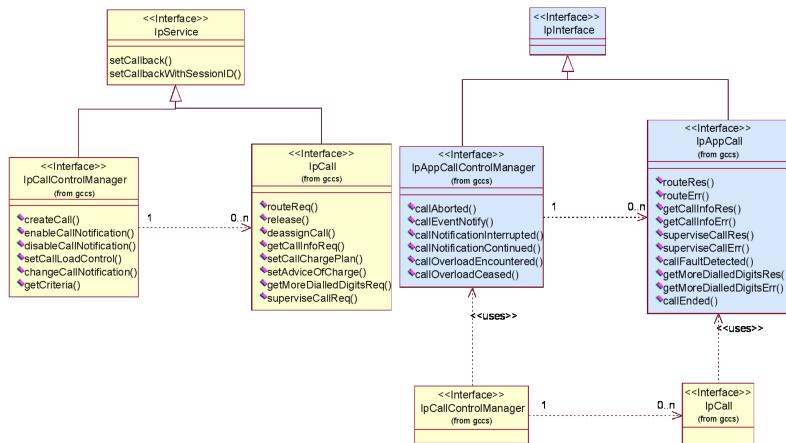


Diagrama de sequência para a interface CallControl

- Classe IpAppLogic
 - Onde se encontra a lógica do serviço
 - Faz pedidos
 - Criação e libertação da chamada (2,10)
 - Estabelecimento de ligações (5,8)
 - Recebe notificações de eventos (6,9)
- Classe IpAppCall
 - Recebe notificações/resultados da parte rede da interface (IpCall)
 - Envia notificações/resultados à lógica de serviço
- Classes IpAppCallControlManager e IpCall
 - Recebe, pedidos da lógica de serviço e da parte aplicação das interfaces
 - Enviam notificações/resultados à parte aplicação das interfaces

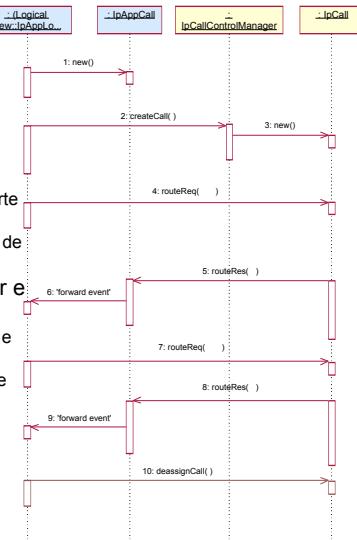
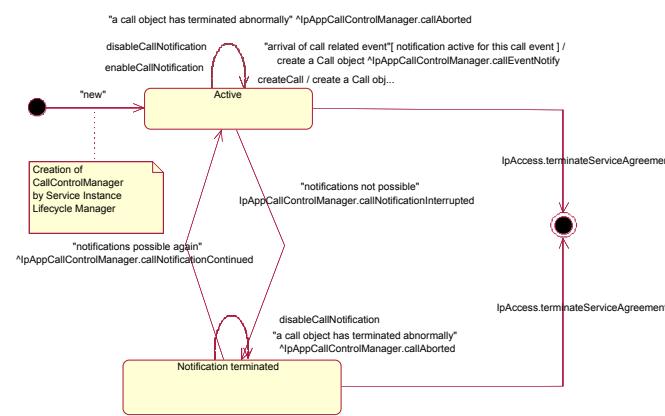


Diagrama estados da classe *IpCallControlManager*



O Network Resource Gateway (NRG) da Ericsson

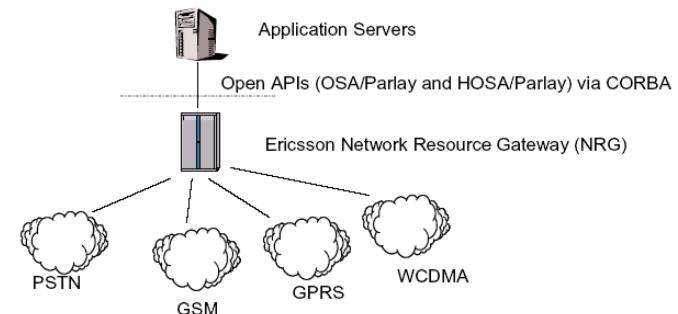
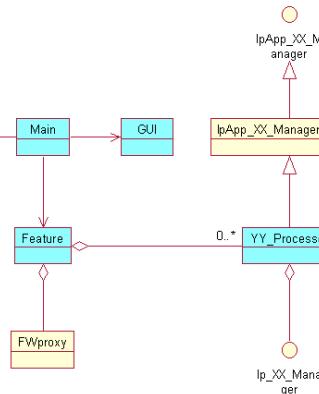


Diagrama de classes das aplicações exemplo do SDK da Ericsson

- Estrutura geral
 - Lógica da aplicação distribuída por várias classes
- Classe Main
 - Responsável por lançar as outras classes (interacção com o FWproxy)
- Classe GUI
 - Interacção com o gestor da aplicação (start, stop, ações)
- Classe Feature
 - Onde se encontra a lógica do serviço
- Classes YY_Processor
 - Abstraem da classe Feature detalhes
 - Pode haver mais de um tipo de YY_Processor numa mesma aplicação
- Classe FWproxy
 - Classe que abstrai alguns dos detalhes da interacção com a Framework (ex., autenticação, SLAs)
 - Permite a obtenção e libertação de service managers



A classe Main das aplicações exemplo

- Classe que abstrai alguns dos detalhes da interacção com a Framework (ex., autenticação, SLAs)
- Permite a obtenção e libertação de service managers
- Alguns métodos chave


```

// Criação de uma instância de FWproxy,
// interacção com a Framework
FWproxy (Properties aProps)
// Obter um service manager
public IpService
obtainSCF (String aSCFName)
// Libertar recursos
void releaseSCF (IpService aSCF)
// Libertar os recursos da Framework
usados
public void endAccess ()
```

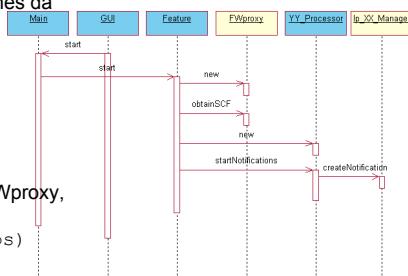
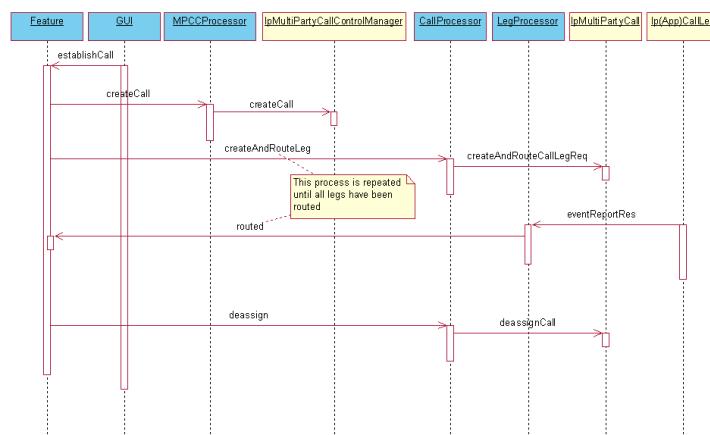


Diagrama de sequência da aplicação exemplo *WebDial* do SDK da Ericsson



Parlay e os Serviços na Web (Web Services): Motivação

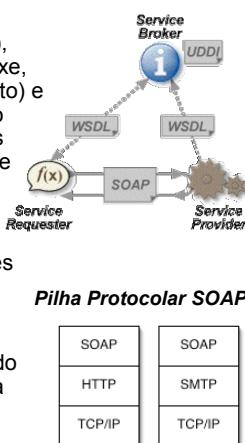
• *Ideia chave:*

- Utilizar as tecnologias associadas à Web para a criação/utilização de serviços
A escrita de aplicações de telecomunicações tem uma semântica simples e semelhante a outros serviços na Web.
- A interacção entre uma aplicação utilizando um Parlay Web Service e um servidor implementando um Parlay X Web Service é efectuada através da troca de mensagens baseadas em XML.
- Dois tipos de actividades:
 - Parlay Web Services (definição em WSDL das interfaces Parlay)
 - Parlay X (solução totalmente Web, abandono de alguns paradigmas)

Web Services (tutorial breve): Arquitectura

Elementos da arquitectura:

- **Fornecedores de serviços (service providers)**, Fornecem um serviços definidos por uma sintaxe, num determinado SAP (ex., endereço IP + porto) e acessível através de um determinado protocolo (ex. SOAP). Estas características são descritas utilizando WSDL e anunciamos a mediadores de serviços.
- **Mediadores de serviços (service brokers)** Recebem registos de serviços por parte de fornecedores e pedidos por parte de utilizadores de serviços fazendo o emparelhamento entre ambos.
- Clientes de serviços. Fazem a descoberta dos prestadores dos serviços desejados consultando mediadores de serviços. Após essa descoberta utilizam esses serviços de acordo com a sua descrição fornecida (em WSDL).



WSDL: Web Services Description Language (v1.1)

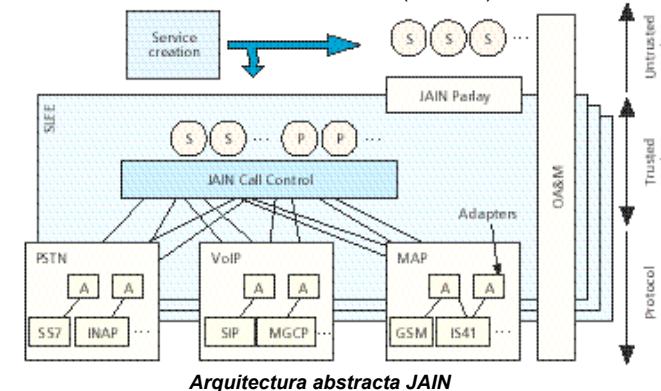
- WSDL define **serviços** através de colecções de portos (**endpoints**).
- Esta definição é independente da sua implementação prática (formato das mensagens e protocolos utilizados).
- Elementos do WSDL (utilização de XML):
 - **Types**: definição de tipos de dados simples e complexos
 - **Messages**: descrição **abstracta** dos dados trocados na prestação de um serviço, composta por várias **parts** (ex., header, body)
 - **Operations**: descrição **abstracta** das ações suportadas por um serviço
 - Definida pelas mensagens dos tipos: **Input**, **Output**, **Fault**
 - Dependendo do dos tipos de mensagens utilizadas podem ser definidos quatro modelos de comunicação:
 - **One-way**, **request-response**, **solicit-response**, **notification**
 - **PortType**: colecção de operações suportadas num ou mais serviços
 - **Binding**: descrição do formato de dados e protocolos usados na implementação de um **PortType**
 - **Port**: um **endpoint** definido como a combinação de um **binding** e um endereço
 - **Service**: colecção de **endpoints** relacionados

Documentos Parlay X (3GPP)

- TS [29.199-01](#) Open Service Access (OSA); Parlay X web services; Part 1: Common .
- TS [29.199-02](#) Open Service Access (OSA); Parlay X web services; Part 2: Third party call .
- TS [29.199-03](#) Open Service Access (OSA); Parlay X web services; Part 3: Call notification .
- TS [29.199-04](#) Open Service Access (OSA); Parlay X web services; Part 4: Short messaging .
- TS [29.199-05](#) Open Service Access (OSA); Parlay X web services; Part 5: Multimedia messaging .
- TS [29.199-06](#) Open Service Access (OSA); Parlay X web services; Part 6: Payment .
- TS [29.199-07](#) Open Service Access (OSA); Parlay X web services; Part 7: Account management .
- TS [29.199-08](#) Open Service Access (OSA); Parlay X web services; Part 8: Terminal status .
- TS [29.199-09](#) Open Service Access (OSA); Parlay X web services; Part 9: Terminal location .
- TS [29.199-10](#) Open Service Access (OSA); Parlay X web services; Part 10: Call handling .
- TS [29.199-11](#) Open Service Access (OSA); Parlay X web services; Part 11: Audio call .
- TS [29.199-12](#) Open Service Access (OSA); Parlay X web services; Part 12: Multimedia conference .
- TS [29.199-13](#) Open Service Access (OSA); Parlay X web services; Part 13: Address list management .
- TS [29.199-14](#) Open Service Access (OSA); Parlay X web services; Part 14: Presence .
- TS [29.199-15](#) Open Service Access (OSA); Parlay X web services; Part 15: Message Broadcast
- TS [29.199-16](#) Open Service Access (OSA); Parlay X web services; Part 16: Geocoding and Mapping .
- TS [29.199-17](#) Open Service Access (OSA); Parlay X web services; Part 17: Application driven Quality of Service (QoS)

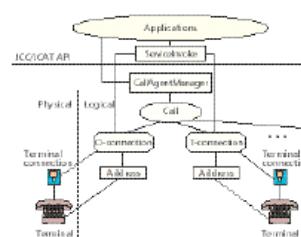
JAIN: Java API for Integrated Networks

- Conjunto de **API Java** aberta, com acesso a “funções” de rede por forma a permitir o desenvolvimento de serviços, potenciando a sua portabilidade, convergência e segurança.
- Assume núcleo da rede como sendo IP (ou ATM)



Call Control (JCC)/Coordination and Transactions (JCAT)

- Modelo para as chamadas (*call model*) em que a “rede” é vista como uma máquina virtual.



Aplicação JAIN (JCC/JCAT) a serviço sobre telefonia

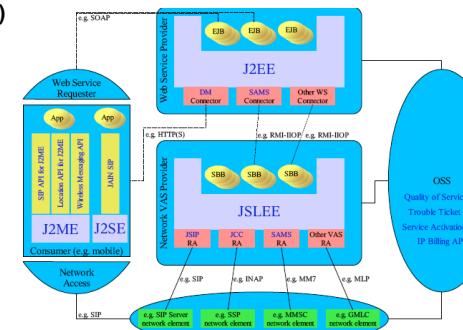
JAIN no contexto das redes e serviços de comunicações

- **Java Service Logic Execution Environment (JSLEE)**: núcleo da prestação de serviços permitindo que aplicações ou *Service Building Blocks* (*SBB*) acedam e manipulem recursos da rede.

• Resource Adaptors (RA)

• Service Building Blocks (SBB)

- Definição de APIs para a gestão da rede e serviços



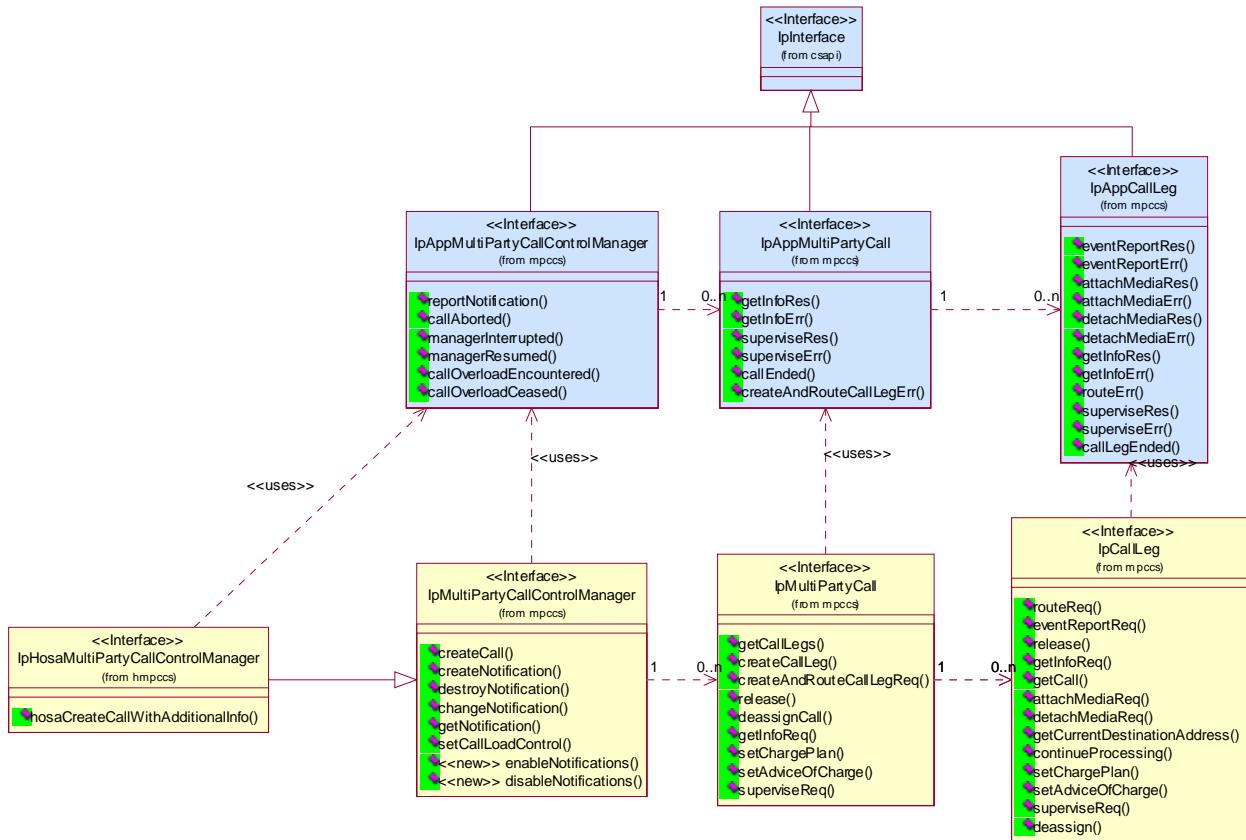
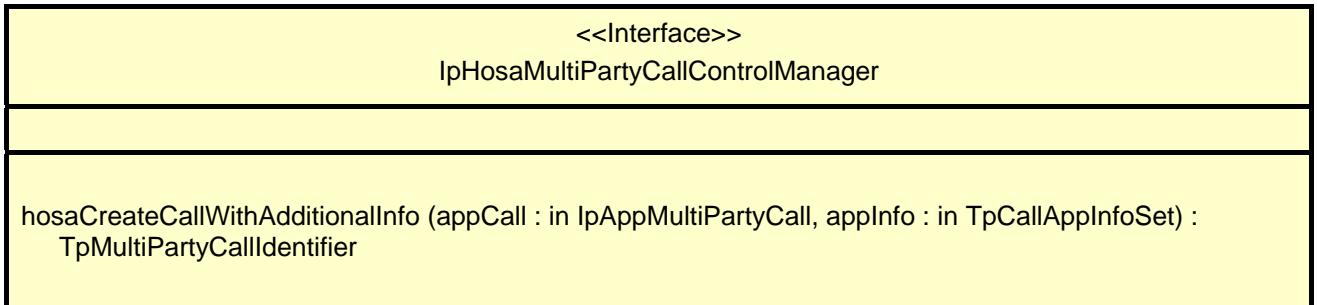


Figure: H-OSA Multi Party Call Control

5.3 H-OSA Multi-Party Call Control Interface Classes

5.3.1 Interface Class IpHosaMultiPartyCallControlManager

Inherits from: **IpMultiPartyCallControlManager**.



Method

hosaCreateCallWithAdditionalInfo()

This method is used to create a new call object. An **IpAppMultiPartyCallControlManager** should already have been passed to the **IpMultiPartyCallControlManager**, otherwise the call control will not be able to report a `callAborted()` to the application (the application should invoke `setCallback()` if it wishes to ensure this).

Returns **callReference**: Specifies the interface reference and sessionID of the call created.

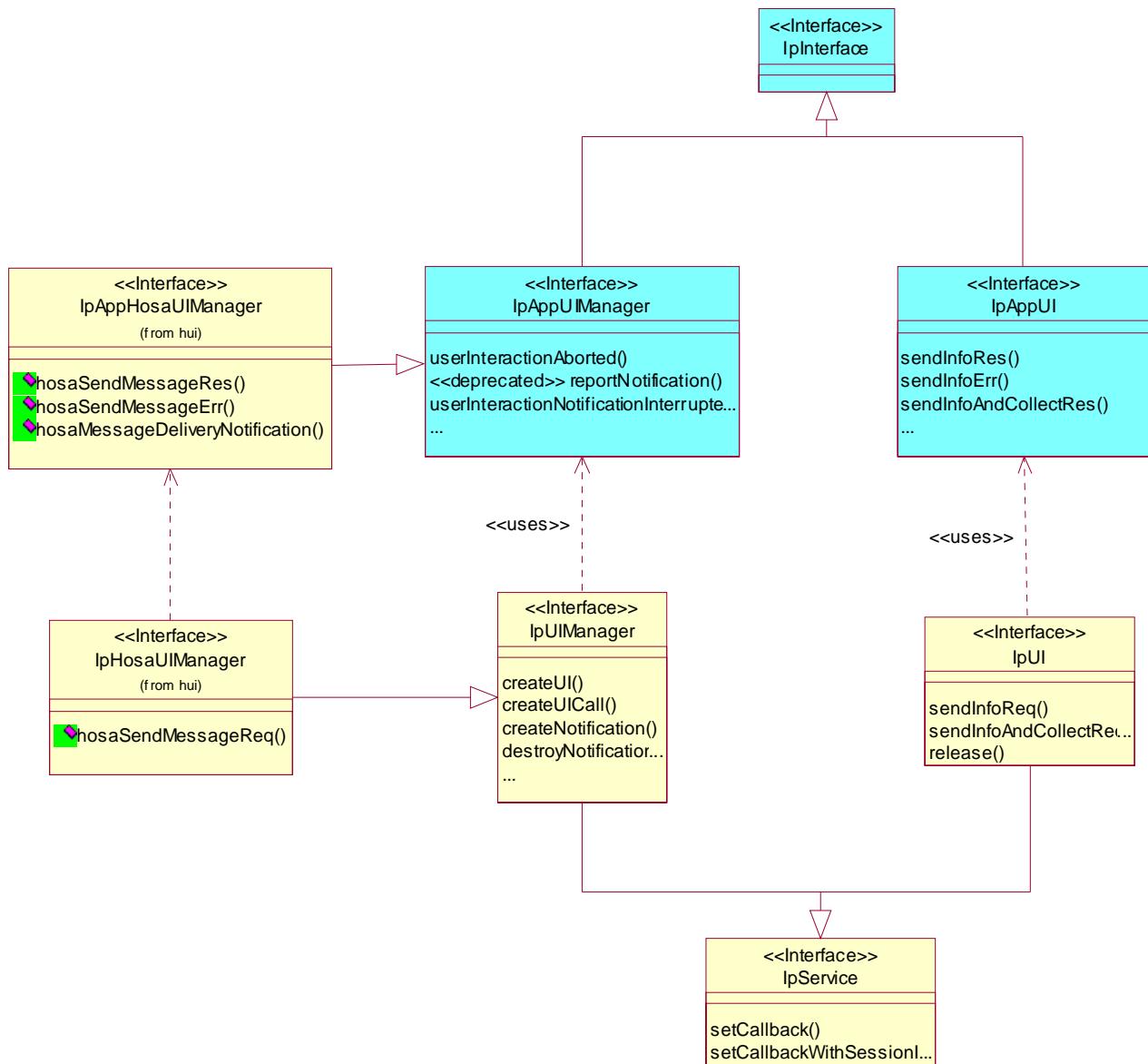


Figure: H-OSA Generic User Interaction Package Overview

5.3 H-OSA Generic User Interaction Interface Classes

5.3.1 Interface Class IpHosaUIManager

Inherits from: [IpUIManager](#).

This interface is the 'service manager' interface for the H-OSAGeneric User Interaction Service and provides the management functions to the H-OSA Generic User Interaction Service.

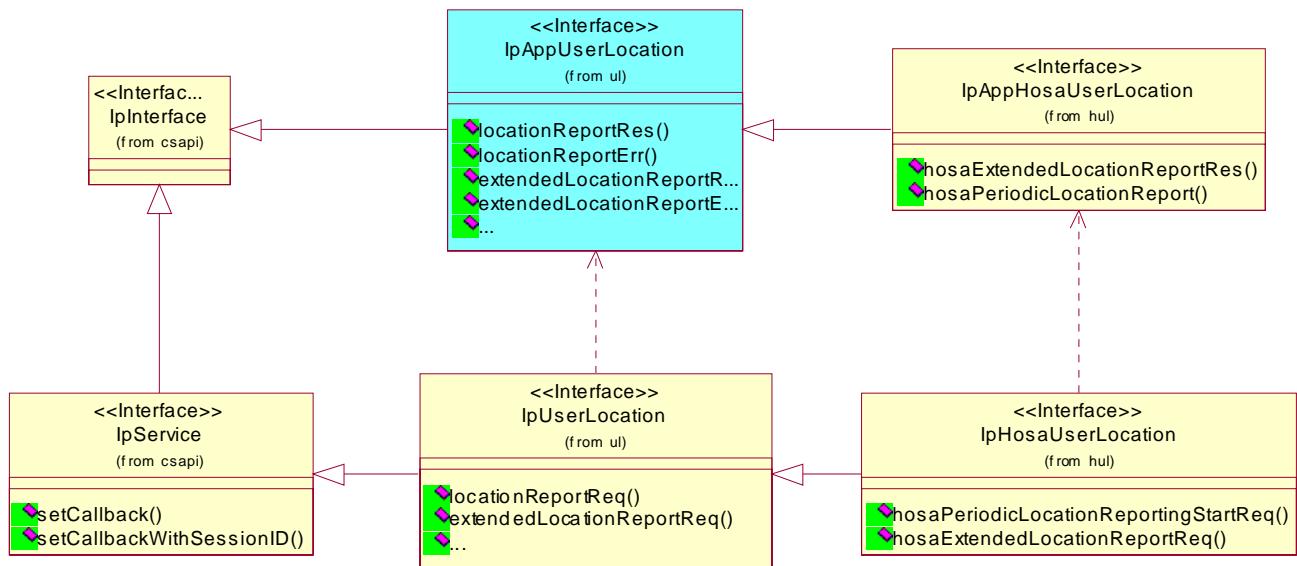


Figure: H-OSA User Location Class Diagram

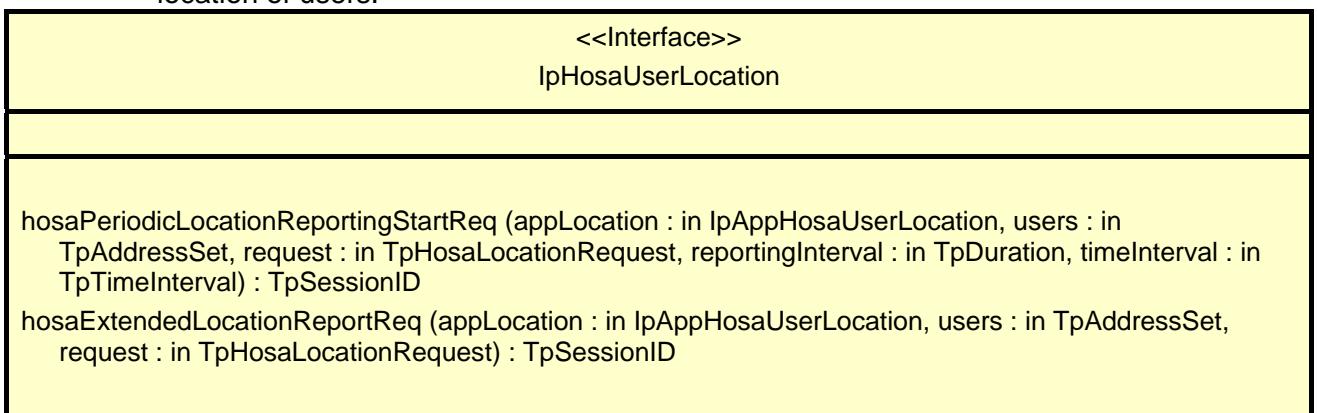
5.3 H-OSA User Location Interface Classes

5.3.1 Interface Class **IpHosaUserLocation**

Inherits from: **IpUserLocation**.

This interface is the 'service manager' interface for the User Location Service.

The user location interface provides the management functions to the user location service. The application programmer can use this interface to obtain the geographical location of users.



Method

hosaPeriodicLocationReportingStartReq()

Request of periodic reports on the location for one or several users.

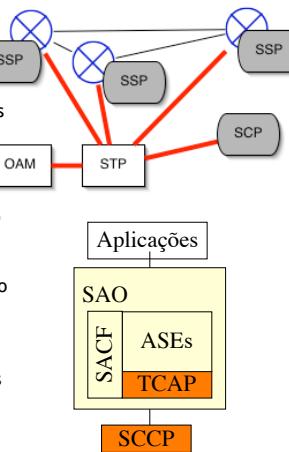


Instituto Universitário de Lisboa
Lisbon University Institute

Sinalização

Motivações e Aplicações: Plano físico na IN

- O plano físico identifica as entidades físicas que implementam as entidades funcionais e os protocolos que permitem a troca de informação entre as entidades físicas.
- As relações existentes entre as entidades funcionais são:
 - SCF-SSF (D)
 - SCF-SRF (E)
 - SCF-SDF (F)
 - São relações do tipo pergunta-resposta ou notificação
- Quando as entidades funcionais se encontram implantadas em entidades físicas distintas o fluxo de informação definido no plano funcional repartido é implementado no plano físico pelo protocolo de aplicação de rede inteligente: *INAP (Intelligent Network Application Protocol)*.
- O INAP utiliza para o seu transporte o SS7, sendo as suas mensagens encapsuladas em mensagens do protocolo *TCAP (Transaction Capabilities Application Protocol)* que por sua vez utiliza o *SCCP: Signalling Connection Control Part* do SS7.

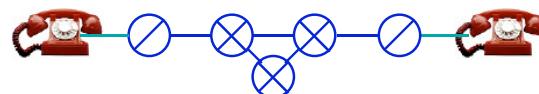


Funcionalidade e evolução da sinalização

- Necessidades e evolução
 - Até 1890: aviso do operador na central de comutação de um pedido de chamada
 - De 1890 (Strowger) a 1976: estabelecimento (comutação) e aviso de chamadas, taxação.
 - (1950 - Introdução da *direct distance dialing - DDD*)
 - (1960 - Introdução da *international direct distance dialing - IDDD*)
 - Desde 1976: digitalização total: sinalização por canal comum
 - Separação entre os circuitos da chamada e de sinalização
 - Serviços suplementares (ex. Identificação do chamador)
 - Suporte para a troca de fluxos de informação entre elementos da IN
 - Suporte para a sinalização de/para redes móveis (MAP e CAP são transportados sobre SS7)

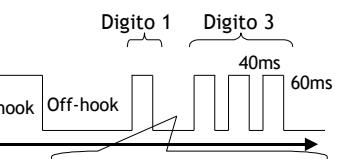
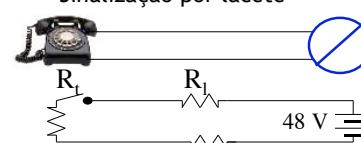
Tipos de sinalização

- Sinalização entre o terminal do assinante e o seu nó de comutação (*subscriber signaling*):
 - Marcação por lacete
 - Marcação por multifreqüência
 - Sistema de sinalização digital do assinante (DSS)
- Sinalização entre nós comutadores (*interchange signaling*):
 - Sinalização por canal associado
 - Sinalização por canal comum
 - Sistemas de sinalização n.o 6 e n.o 7 (SS7)

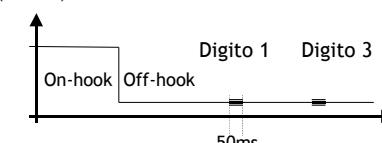
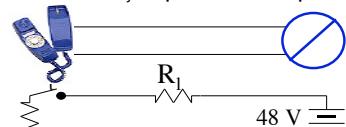


Sinalização entre o terminal do assinante e o seu nó de comutação

- Sinalização por lacete



- Sinalização por multifreqüência (DTMF)



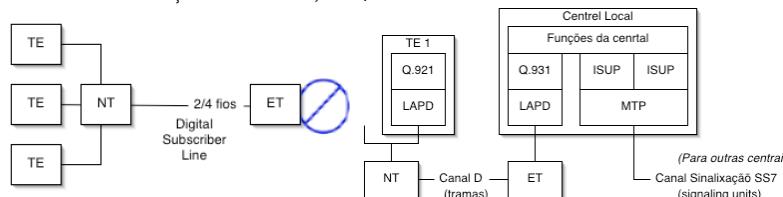
	F1	F2	F3	F4
f1	1	2	3	A
f2	4	5	6	B
f3	7	8	9	C
f4	*	0	#	D

$f1 = 1209 \text{ Hz}$
 $f2 = 1336 \text{ Hz}$
 $f3 = 1447 \text{ Hz}$
 $f4 = 1633 \text{ Hz}$

$f1 = 697 \text{ Hz}$
 $f2 = 770 \text{ Hz}$
 $f3 = 852 \text{ Hz}$
 $f4 = 941 \text{ Hz}$

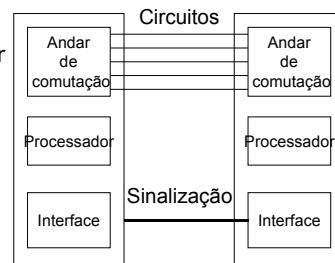
Sinalização entre o terminal do assinante e o seu nó de comutação (DSS n.º 1)

- Sinalização digital no lacete local
 - Introduzida com a RDIS (entre o assinante RDIS a sua central local)
 - Capacidade da DSL (acesso básico 2B+D): 144kbps
 - 144kbps = (2*B channel) 2*64kbps + (D channel) 16kbps
 - Canal D usado (normalmente) para sinalização utilizando a norma DSS1,
 - Digital Subscriber Signaling 1 - sistema de sinalização orientado às mensagens
 - Arquitectura de dois níveis: ligação de dados (LAPD) e rede (Q.931)
 - LAPD: O canal D suporta vários *data link connections* simultâneas
 - Tramas: endereçamento, tipo de trama (I, S, U), controlo de erros
 - Q.931: Diferentes tipos de mensagens estabelecimento, progresso, terminação de chamadas; e acções durante a chamada



Sinalização entre centrais: canal comum

- Na sinalização por canal comum um canal de sinalização é partilhado por vários circuitos de voz
- **Principais características:**
 - Diminuição do nº de circuitos
 - Aumento da velocidade na interacção com o processador
 - Informações mais ricas
 - Melhoria nos tempos de resposta
 - Melhoria na fiabilidade e menos possibilidade de fraude
 - Melhor interface com os órgãos de controlo
 - Evita interferências
 - Redução de custos de instalação e exploração e manutenção.
- **Desvantagens:**
 - Não há teste automático do canal de voz
 - Falhas no canal de sinalização afectam um grande nº de circuitos

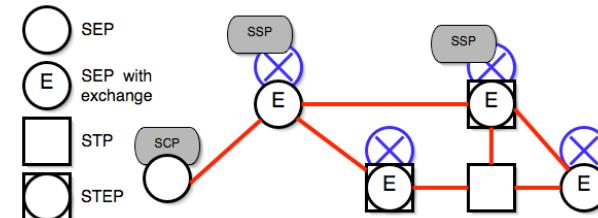


Sinalização entre centrais: canal associado

- Unica forma de sinalização entre centrais até 1976
- Existente conjuntamente com diferentes tipos de multiplexagem (FDM, TDM) e transmissão (análogica e digital)
- Na sinalização por canal associado existe um canal de sinalização reservado para cada circuito de voz, usualmente partilhando (associado) ao canal de voz,
- As funções da sinalização por canal associado são:
 - A sinalização de linha cuja principal função é estabelecer uma ligação e supervisionar a mesma depois de estabelecida.
 - A sinalização entre registadores destinada à transmissão de toda a informação numérica.
- A sinalização pode ser:
 - Por lacete ou equivalente, utilizando um circuito dedicado
 - Por frequência na banda, se for usada a gama dos 300-3400Hz aproveitando os amplificadores de voz, exemplo CCITT nº4 2040-2400Hz para sinalização de linha e entre registadores bidirecional.
 - Por frequência fora da banda se estiver fora da faixa dos 300 aos 3400Hz

Sinalização canal comum: conceitos

- Aparecimento do conceito de rede de sinalização ("paralela" à rede de transmissão usada para os "dados" do serviço)
- Rede sinalização composta por:
 - **Pontos de sinalização (signaling point - SP):** entidade na rede de sinalização à qual estão ligado(s) circuito(s) de sinalização
 - Tipos de pontos de sinalização
 - Signaling end point - SEP:** ponto extremo num caminho de sinalização (gera e consome informação de sinalização).
 - Alguns pontos extremos de sinalização podem acumular essa função com a função de comutadores na rede de circuitos de troncos, mas não necessariamente (e.g., um SCP).
 - Signaling transfer point - STP:** ponto de sinalização intermédio num caminho de sinalização cuja função é apenas a transferência de mensagens
 - Signaling transfer and end point - STEP:** ponto de sinalização que é um ponto extremo numas relações de sinalização e um ponto de transferência noutras

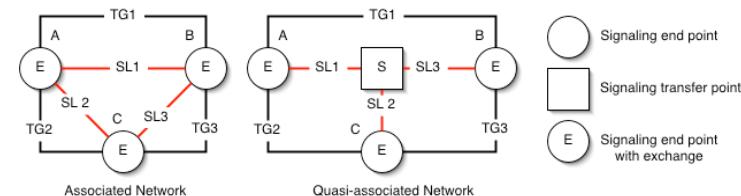


Sinalização canal comum: conceitos

- **Ligação de sinalização (signaling link):** Infraestrutura de transporte bidirecional que interliga dois nós da rede de sinalização, pontos de sinalização adjacentes (SP). Normalmente operam em partilha de carga - redundância. Definidas pelos níveis 1 e 2 do MTP.
- **Feixe de ligações de sinalização (signaling link set):** Conjunto de ligações de sinalização que interligam dois SP utilizados como um módulo operando (normalmente) em regime de partilha de carga).
- **Relação de sinalização (signaling relation):** existe entre quaisquer dois pontos extremos de sinalização (signaling end points) que **necessitem** de trocar informação de sinalização entre si.
Diz-se que existe uma relação de sinalização entre dois SEP se for possível estabelecer comunicação entre os User Part correspondentes.
- **Rota de sinalização (signaling route):** Caminho pré-determinado (sucessão de ligações e pontos de transferência de sinalização - STP), percorrido por uma mensagem de sinalização entre o SEP origem e o SEP destino para uma dada relação de sinalização.
- **Grupo de ligações de sinalização (signaling link group):** Conjunto de ligações de sinalização com as mesmas características dentro de um feixe (por exemplo a cada conjunto corresponde uma relação de sinalização com características diferentes).

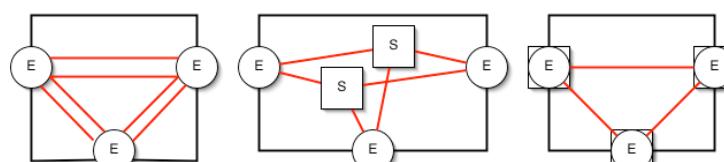
Modos de sinalização por canal comum

- *O modo de sinalização classifica a associação entre o caminho percorrido por uma mensagem de sinalização e a relação de sinalização a que diz respeito*
- **Modo associado:** cada rota corresponde a uma ligação de sinalização à qual está *associada* uma relação de sinalização. A ligação de sinalização SL1 corresponde à relação A,B e só transporta a informação de sinalização correspondente aos circuitos de TG1 (as mensagens para uma dada relação de dois SP adjacentes são transferidas através do feixe directo que os interliga)
- **Modo quasi-associado:** o caminho seguido por uma mensagem para uma dada relação de sinalização é constituído por duas ou mais ligações em *tandem* (passando por um ou mais STP). Este caminho é fixo em cada instante. Cada ligação de sinalização transporta informação de sinalização respeitante a várias ligações.



Redundância e balanceamento de carga na sinalização por canal comum

- **Redundância** necessária por forma a que falhas num circuito de sinalização não afectem um grande número de circuitos
- **Balanceamento de carga** necessário por forma a que o desempenho do sistema se mantenha em níveis aceitáveis em situações de elevado trágefo de sinalização em algumas ligações
- **Técnicas:**
 - Utilização de feixes de ligações de sinalização
 - Utilização de grupos de ligações de sinalização
 - Utilização de pontos de sinalização terminais como pontos de transferência



Normalização da sinalização por canal comum

- Necessidade de normalização por forma a ser possível a interligação de sinalização entre diferentes redes
- Na sinalização por canal comum um canal de sinalização é partilhado por vários circuitos de voz
- A sinalização nº 6 e a nº7 do CCITT.
 - Nestes sistemas são considerados 4 níveis funcionais:
 - *O nível de ligação* - constituído pelo suporte físico de transmissão e respectivas terminações
 - *O nível função de canal comum* - responsável pela gestão da troca de informação. Este nível implementa as funções de delimitação de tramas, sincronização, detecção e correcção de erros.
 - *O nível de orientação de mensagens* - responsável pelo encaminhamento das mensagens de e para o respectivo subsistema de utilizador, e pela gestão da rede.
 - *O nível do subsistema de utilizador* - diferentes instâncias adequadas às aplicações de diferentes redes (PSTN, ISDN, IN)
 - A informação é trocada sobre a forma de mensagens ("pacotes") com um nº variável de campos, como por exemplo:
 - Informação útil (e.g., origem, destino e dados)
 - Dados de sincronização e numeração de controlo.
 - Informação redundante destinada à detecção e correcção de erros

Sistemas de sinalização SS6 e SS7

O Sistema de Sinalização n.o 6

- O sistema de sinalização nº 6 foi definido em 1972 para a rede internacional utilizando canais a 2.4 kbit/s para aplicações analógicas (no que respeita ao transporte das chamadas).
- Posteriormente surgiram versões a 4 e 56 kbit/s para aplicações digitais bem como extensão a redes nacionais.
- As mensagens são de tamanho fixo e relativamente pequeno, 28 bytes

O Sistema de Sinalização n.o 7

- O sistema de sinalização nº7 do CCITT foi desenvolvido entre 1980 e 1983 com a possibilidade de operar tanto a nível nacional como internacional (Yellow Book em 1981)
- Prevê a sua aplicação em redes digitais e analógicas.
- As mensagens são de comprimento variável o que se traduz numa optimização de recursos.

Sistema de sinalização SS7

O Sistema de Sinalização n.o 7

- O Sistema de sinalização nº 7 é um sistema de sinalização por canal comum universal e normalizado a nível internacional.
- Consiste num protocolo de comunicação de dados para transferência fiável de informação entre processadores numa rede de telecomunicações.
- Responde não só às necessidades de sinalização para os serviços telefónicos mas também para outros serviços em redes de telecomunicações (e.g., a IN e na interligação de redes moveis)

Objectivos do Sistema de Sinalização n.o 7

- Optimizada para operar em redes digitais de telecomunicações em conjunto com centrais SPC (controladas por computador).
- Capaz de responder às necessidades actuais e futuras de transferência de informação em redes de telecomunicações, para o controlo de chamada, sinalização, gestão e manutenção.
- Capaz de assegurar uma correcta troca de informação, sem erros nem duplicações

Sistema de sinalização SS7

Outras características do Sistema de Sinalização n.o 7

- Sistema de sinalização por canal comum com um vasto campo de aplicação não limitada à sinalização telefónica.
- Implementa uma rede para sinalização entre nós de uma rede de telecomunicações que não é mais do que uma rede de dados que pode também ser utilizada para outros fins
 - Funcionalidades de ligação de dados (controlo erros/fluxo) e rede (encaminhamento)
- Existência de diversos tipos de utilizadores da rede de sinalização comum, com funções muito diferentes, admitindo a existência de novos utilizadores que venham a ser definidos para aplicações particulares
 - Associado à existencia de diferentes implementações do *User Part*
- Sistema de Sinalização modular flexível que permite ser configurado de acordo com a aplicação ou aplicações a que se destina

Sistema de sinalização SS7

Características gerais/requeridas para o sistema SS7

- Rede de comutação de mensagens
- Alta disponibilidade:
 - Redundância de ligações
 - Mecanismos integrados de gestão da rede
- Alta fiabilidade:
 - Detecção de erros
 - Correcção de erros
 - Reencaminhamento automático em caso de falha
- Versatilidade
 - Estrutura dependente da aplicação pretendida

Componentes da rede

- Pontos de sinalização (Signalling Points - SP)
- Ligações de Sinalização (Signalling Links - SL)

*As ligações de sinalização ligam os pontos de sinalização.

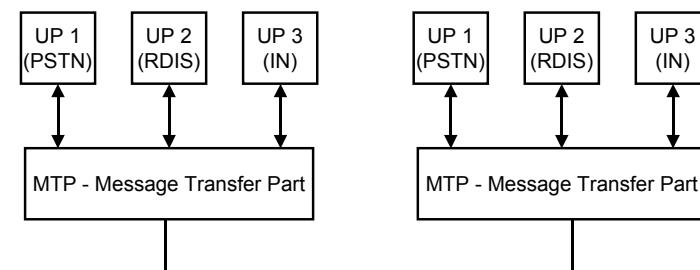
Sistema de sinalização SS7

Campos de aplicação do Sistema de Sinalização n.o 7

- Sinalização na rede telefónica tradicional -PSTN
- Sinalização não relacionada com o controlo do circuito. Permite troca de informação entre as duas centrais no extremo de uma chamada, (ex: informação que a chamada foi redirecionada, identificação de assinante).
- Sinalização para a RDIS
- Sinalização de/para redes móveis
- Transferência de informação entre nós de redes de telecomunicações e centros especializados do processamento de dados para controlo de serviços ou tratamento de informação administrativa.
- Transferência de informação entre de redes e centros de operação e gestão de rede

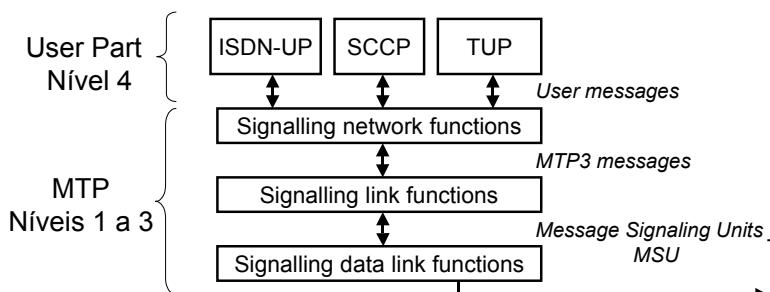
Arquitectura do SS7

- Composta por dois blocos funcionais
 - MTP- Message Transfer Part que implementa um sistema flexível de transporte de informação entre 2 nós da rede de sinalização.
 - User Parts - entidade funcional utilizadora da rede de sinalização, instâncias adaptadas às necessidades de cada tipo de rede.



Hierarquia protocolar do SS7: níveis funcionais

- Nível 1 (Signalling data link) - Suporte do canal de sinalização. Define as características físicas, eléctricas e funcionais das ligações de dados de sinalização.
- Nível 2 (Signalling link) - Define as funções e procedimentos para a transferência de mensagens numa ligação de sinalização. Virtualiza o canal físico. Em conjunto com o nível 1 suporta uma ligação fiável entre dois nós da rede.
- Nível 3 - Define as funções de rede comuns às diferentes ligações de sinalização Signalling Network Functions.
- Nível 4 - É constituído pelos diferentes utilizadores da rede de sinalização (User Part). Cada um destes utilizadores define funções e procedimentos próprios de acordo com as suas características.

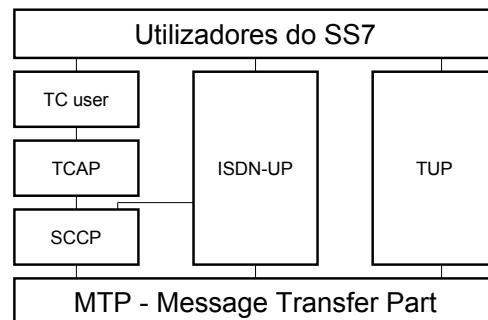


Exemplos de instâncias no User Part

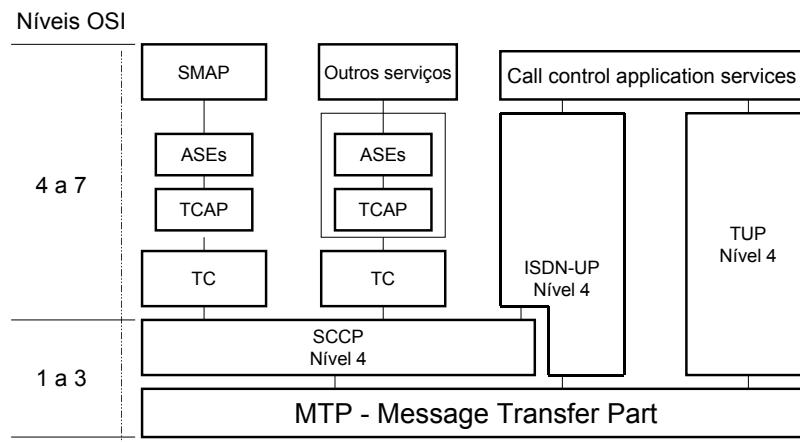
- TUP (Telephone User Part): Define as funções de sinalização necessárias para utilizar o SS7 como sistema de sinalização da rede telefónica internacional.
- ISUP (ISDN User Part): Define as funções necessárias para o fornecimento de serviços comutados e "User Facilities" para aplicações vocais e não vocais numa RDIS.
- DUP (Data User Part) Rec. X61 para controlo de circuitos comutados de dados entre centrais (muito pouco usado).
- SCCP (Signalling Connection Control Part): Tem funções adicionais ao MTP para permitir o fornecimento de serviço quer não orientados à ligação quer orientados à ligação na rede de sinalização fornecendo funções adicionais de encaminhamento

Exemplos de utilizadores do SCCP

- ISUP (ISDN User Part): Usa o SCCP para sinalização ponto a ponto.
 - TCAP (Transaction Capabilities Applications Part): Permite estabelecer comunicação para sinalização não associada a circuitos entre dois nós da rede (i.e., podem não ser comutadores ou nós do PSTN).
- Baseada num serviço não orientado à ligação fornecido pelo SCCP.



Comparação entre o SS7 e o modelo OSI



SCCP+MTP = NSP - Network Service Part: fornece os serviços definidos para os níveis 1 a 3 do modelo OSI

Pontos de sinalização no SS7

- Entidades onde existem o MTP e/ou as User Parts do SS7.
- Podem ou não ser simultaneamente nós de outras redes. (ex: comutador telefônico - *exchange*).
- Um ponto de sinalização que só contenha a MTP é denominado: Ponto de transferência de sinalização (*Signalling Transfer Point - STP*).
- Um nó físico pode comportar mais do que um ponto de sinalização.
- Um ponto de sinalização é identificado por um código (point code - PC) único de 14 bits.
- Um ponto de sinalização pode funcionar nos seguintes modos:
 - Originante
 - Destinatário
 - Transferência (STP ou SP com função STP)

Identificação de pontos de sinalização no SS7

- Os pontos de sinalização são identificados através de códigos de ponto (*point code*)
 - Pelo menos um nó em cada país deverá ter hipótese de funcionar como ponto de transferência para tráfego internacional, de forma a garantir flexibilidade total de encaminhamento. (Podem existir no máximo 8 por cada rede atribuída ao país - 3 bits *V*)

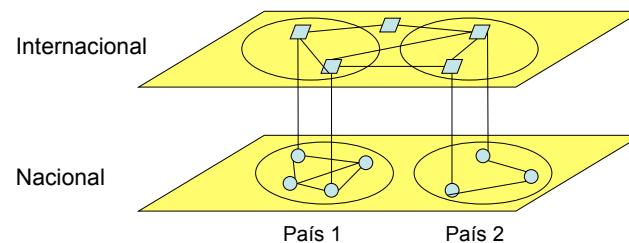
Código do ponto de sinalização internacional (CPSI)		
Z (3 bits)	U (8 bits)	V (3 bits)
Id. de zona	Id. de rede	Id. de ponto
(ou) Código da zona/rede de sinalização		

Z . Zonas Mundiais	
Europa	2-UUU
América N C	3-UUU
Ásia	4-UUU
Oceânia	5-UUU
África	6-UUU
América Sul	7-UUU

Portugal	2-136 a 2-139
EUA	3-020 a 3-059
Ex URSS	2-100 a 2-119

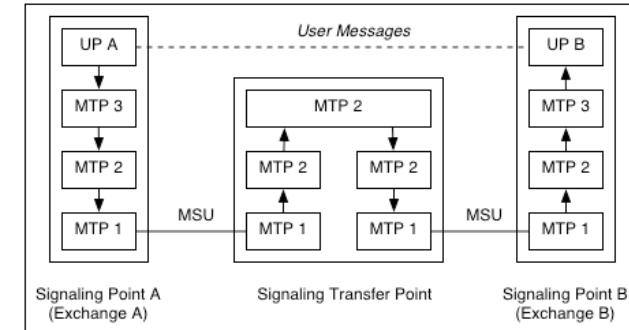
Estrutura da rede de sinalização

- Existe uma independência estrutural entre a rede internacional e as redes nacionais, permitindo:
 - Uma gestão independente entre as redes nacionais e internacional
 - Uma atribuição independente dos Point Codes
 - Opções próprias das redes nacionais.



Transferência de mensagens no SS7

- Formato, sequência, temporização e semântica de mensagens entre entidade pares definidas por **protocolos** (ex., TUP, TCAP)
- Utilização de serviços e encapsulamento de dados entre níveis no mesmo nó.
- Nós de transferência de mensagens (STP) apenas implementam o MTP
- Semelhanças claras com outras redes de dados!*



Estrutura e planeamento da rede de sinalização

- A estrutura da rede de sinalização depende de:
 - Volume de sinalização (redundância)
 - Disponibilidade pretendida (fiabilidade)
 - Estrutura da rede de telecomunicações a controlar
 - Outros aspectos (ex: administrativos)
- Gestão da rede de sinalização
 - É independente da gestão da rede controlada
 - Existem meios automáticos incorporados no MTP
- O planeamento pode ter duas abordagens:
 - Planeamento com base nas relações de sinalização:
 - Rede largamente baseada no modo associado.
 - Estrutura muito próxima (ou idêntica) à rede controlada.
 - Planeamento na perspectiva da rede como um recurso comum capaz de satisfazer as necessidades de sinalização.
 - Rede largamente baseada no modo quase-associado
 - Estrutura independente da rede controlada
 - Melhor aproveitamento do potencial do sistema de sinalização
 - Uso de STPs - Uso de links comuns para relações com baixo volume sinal.
 - Desvantagem: Pode existir duplicação de mensagens em caso de falha
- A capacidade da rede é sempre muito superior ao tráfego oferecido !**

Estrutura e planeamento da rede de sinalização

- Existem alguns pontos recomendados a ter em atenção no planeamento da rede internacional, também aplicáveis às redes nacionais.
 - Minimização da utilização de ligações de sinalização via satélite.
 - Só devem existir dois STPs em cada relação de sinalização na rede internacional, este valor pode ser temporariamente superior em casos de falha.
 - Deve existir sempre redundância nas ligações de sinalização entre dois SPs. O nº de ligações em partilha de carga depende de:
 - Tráfego total de sinalização
 - Disponibilidade de cada ligação individualmente
 - Disponibilidade pretendida entre dois SPs
 - Débito binário das ligações
 - Normalmente existem apenas duas ligações de sinalização entre 2 pontos com uma ocupação média de cerca de 15 a 20%. Deve existir sempre capacidade disponível para transportar o tráfego de outra(s) ligações em caso de falha e haver margens para suportar picos de tráfego.
 - A indisponibilidade de um conjunto particular de rotas de sinalização não deve exceder os 10 minutos/ano.

Estrutura das mensagens de sinalização

- Uma mensagem de sinalização é um conjunto de informação definido nos níveis 3 (MTP) ou 4 (UP) e transferida como uma entidade pelo MTP.
- Informação comum a todas as mensagens:
 - Service Information Octet (SIO):
 - Identificação do utilizador que envia a mensagem
 - Indicação da rede a que pertence a mensagem
 - Etiqueta/rótulo de encaminhamento, (*routing label*)
 - Point Code de origem
 - Point Code de destino
 - Selector da ligação de sinalização (a usar para partilha de carga)

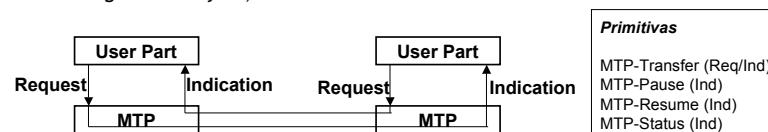


Conjunto de recomendações ITU-T para o SS7

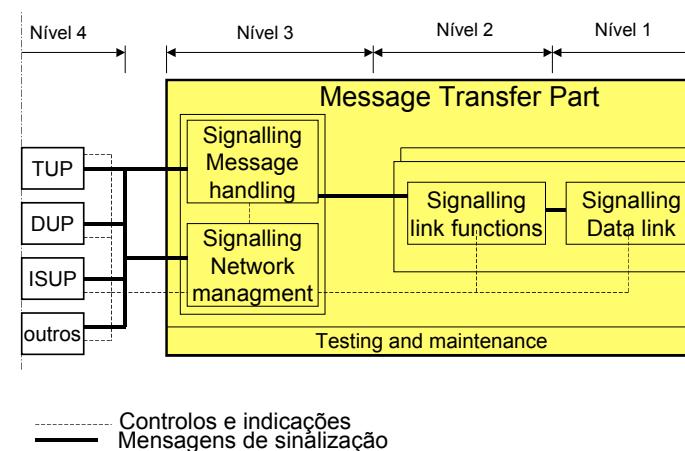
- Message Transfer Part: Q.701 a Q.704, Q.707 e Q.708.
- Telephone User Part: Q.721 a Q.725.
- ISUP: Q.761 a Q.764, Q.766, Q.767 Serviços.
- Data User Part: Q.741 (X.61).
- SCCP - Signalling Connection Control Part: Q.711 a Q.716.
- TC - Transaction Capabilities: Q.771 a Q.775.
- OMAP: Operation Maintenance and Administration Part: Q.750, Q.752 a Q.754, Q.795.
- Estrutura da Rede: Q.705
- Numeração dos "point codes": Q.708.
- Especificações de Teste: Q.780 a Q.787.
- Monitorização da rede SS7: Q.752, Q.791.
- Outros: Q.709.
- Suplementares em ISDN: Q.730

MTP: Message Transfer Part

- Implementa um sistema de transporte fiável para a transferência das mensagens de sinalização.
- Fornece um serviço similar ao de uma rede de comutação de pacotes. Cada mensagem é tratada individualmente e é autónoma (comutação de msgs).
- Inicialmente projectada tendo em vista as necessidades de sinalização para o serviço telefónico (alta disponibilidade e resistência a falhas).
- Para que seja possível a introdução fácil de novos tipos de utilizadores (*User Parts* do SS7) o seu interface com o nível superior é simples e bem definido.
- Não possui mecanismos para:
 - Assegurar a correcta sequência de mensagens no destino.
 - Segmentação e reconstrução de mensagens.
 - Controlo de ligações lógicas.
- Endereçamento limitado (endereço constituído apenas por *Point Codes*)
- Mensagens de tamanho variável (com máximo de informação de utilizador por mensagem: 272 bytes)



Estrutura do Message Transfer Part

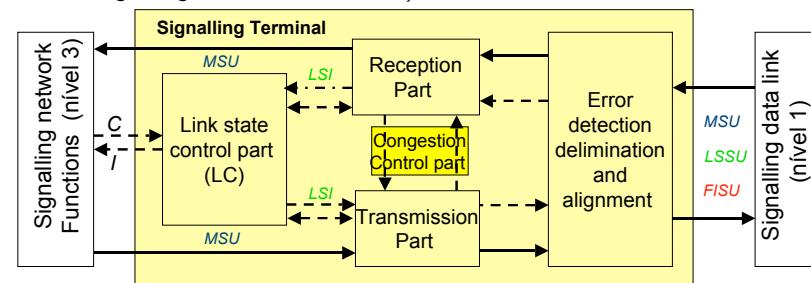


Nível 1 - Ligação de dados de sinalização (Signalling data link)

- Suporte de uma ligação de sinalização (*signalling link*)
- Composto por um canal de transmissão e a interface ao terminal físico de sinalização.
- Canal bidireccional transparente operando em “full duplex” composto por canais de dados unidireccionais entre dois nós adjacentes.
- Dedicados para utilização do SS7.
- Normalmente estabelecido sobre meios de transmissão digitais
 - ex. slots num canal T1/E;
 - mas também pode utilizar meios analógicos.
- Em ligações digitais:
 - A taxa de débito binário não é fixa
 - Normalmente 64kbit/s
 - Mínimo para sinalização telefónica 4.8 kbit/s
 - Implementado por exemplo através de um *slot* em cada trama ou um bit em cada *slot*.

Nível 2 - Ligação de sinalização (Signalling link)

- Define as funções necessárias para a transferência fiável de mensagens de sinalização entre dois nós adjacentes.
- Virtualiza uma ligação de sinalização (*signalling data link*).
- A informação é transferida em unidades de sinalização (*Signal Units*)
- Composto por:
 - Signalling data link - nível 1
 - Signalling terminal - executa funções do nível 2



Funções do nível 2

- Delimitação de tramas
- Alinhamento das unidades de sinalização (sincronização)
- Detecção de erros
- Correcção de erros (por retransmissão)
- Monitorização da taxa de erros na ligação
- Alinhamento inicial da ligação (sincronização e qualidade da ligação)
- Controlo de fluxo (congestionamento do processador)

Tipos de unidades de dados no nível 2

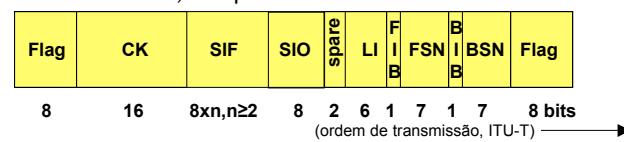
- Unidades de sinalização de Mensagem
MSU, Message Signal Units - $(2 < LI \leq 63)$. ($= 63$ indica ≥ 63 octetos)
- Unidades de sinalização de Estado da ligação
LSSU, Link Status Signal Units - ($LI = 1$ ou 2).
- Unidades de sinalização de enchimento
FISU, Fill-In Signal Units - ($LI = 0$).

Todas as unidades de sinalização tem um número inteiro de bytes

Se $LI = 63$
O comprimento pode ser até 272 bytes

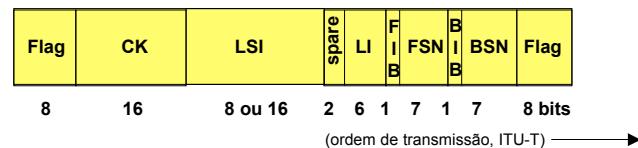
Unidades de sinalização - MSU

- MSU - Unidades de sinalização de mensagem
 - São geradas pelo:
 - nível 3 mensagens de gestão de rede e teste
 - nível 4 - User Parts
 - transporta um máximo de 272 Bytes de informação de utilizador
- Campos do cabecalho da MSU
 - *Flag*, = 0111110
 - *BIB* - Backward indicator bit
 - *BSN* - Backward sequence number
 - *FIB* - Forward indicator bit
 - *FSN* - Forward sequence number
 - *LI* - Length indicator, $2 < LI \leq 64$
 - Mensagem de sinalização vinda do MTP3
 - *SIO* - Service Information Octet
 - *SIF* - Signalling Information Field
 - Ex: Initial Address Message (IAM), Release Message (REL)
 - *CK* - Check Block, campo detector de erros



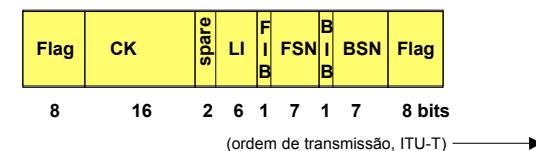
Unidades de estado da ligação - LSSU

- *LSSU - Link state signaling unit*
 - São geradas pelo nível 2:
 - No alinhamento inicial da ligação
 - Durante o período de verificação da taxa de erros da ligação
 - Em casos de falha no terminal de sinalização
 - Em situações de congestão do nível 2
 - *LSI - Link State Information*: Transporta informação sobre o estado da ligação, exemplos:
 - Fora de serviço - SIOS
 - Fora de alinhamento - SIO
 - Alinhamento "Normal" - SIN
 - Alinhamento "Emergência" - SIE
 - Congestão - SIB
 - Estado de isolamento (Processor Outage) - SIPO



Unidades de enchimento - FISU

- *FISU - Fill-in signaling unit*
 - Unidade de enchimento do canal de sinalização
 - Não representam uma fonte de congestionamento (o canal físico é dedicado exclusivamente para a sinalização)
 - São geradas pelo nível 2 quando não existem outras unidades de sinalização para transmitir.
 - Não transporta informação.
 - Serve para:
 - Monitorização contínua da taxa de erros na ligação.
 - Reconhecimento (acknowledge) de unidades de sinalização recebidas



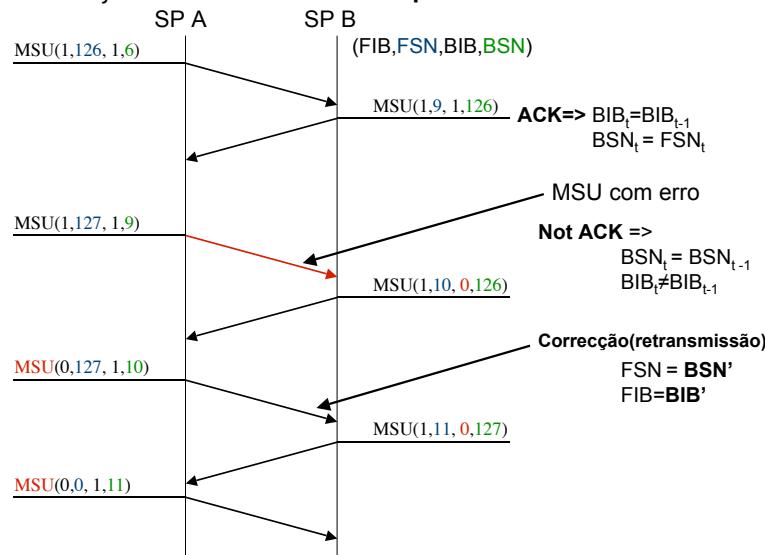
Funções do MTP nível 2

- Delimitação das unidades de sinalização
 - Por bandeiras (tipo HDLC) 01111100
 - Transparência assegurada por inserção/remoção de um 0 após 5 uns seguidos - *bit stuffing (recordar o HDLC!)*
- Detecção de erros
 - É efectuado por um campo de 16 bits (CK - *check bits*) adicionados no final de cada S.U.
- Alinhamento das unidades de sinalização
 - Por reconhecimento de uma bandeira de abertura (não seguida de outra)
 - Teste ao comprimento da S.U. recebida (múltiplo de 8 bits e pelo menos 6 bytes e um máximo de 279 bytes)
 - Se foram recebidos mais de 7 uns seguidos ou mais de 279 bytes entra-se num *modo de contagem de octetos* - para detecção de situação de erro - e todos os bits até à próxima bandeira são descartados.

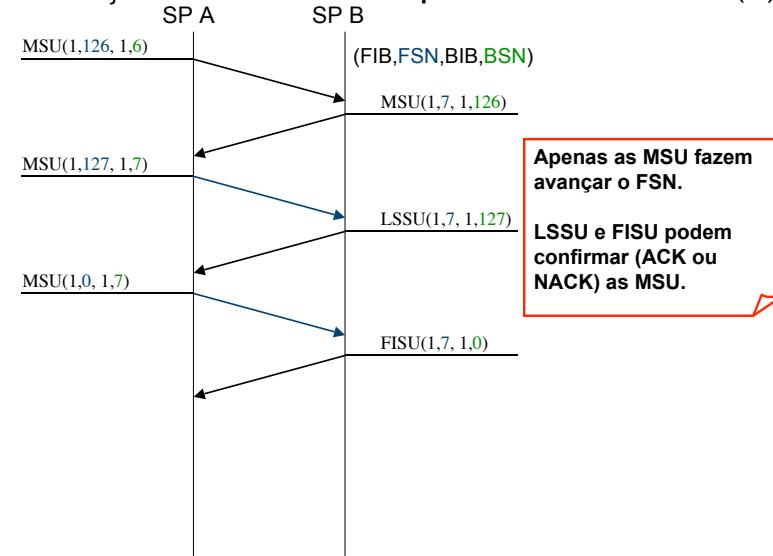
Funções do MTP nível 2: Correcção de erros

- A correcção é efectuada por meio de retransmissão dos S.U. - apenas as MSUs.
- Cada SU tem um número de sequência FSN que é incrementado por cada MSU transmitida. (LSSU e FISU mantêm o FSN da última MSU.) (FSN=0...127).
- A sinalização de sucesso (insucesso) de S.U.s é feita recorrendo a *ack* positivos (negativos).
- Existem dois métodos para a correcção de erros:
 - **Básico**, utilizado quando o tempo de propagação na ligação é menor que 15 ms. Consiste na retransmissão paenias quando for recebido uma não confirmação negativa (NACK).
 - **Retransmissão cíclica preventiva**, utilizado quando o tempo de propagação na ligação é maior que 15 ms. Consiste na retransmissão quando não há MSUs para transmitir ou há muitas mensagens por confirmar. *Neste método não há confirmações negativas.*
- Ambos os métodos requerem que exista um *buffer* para guardas as mensagens para as quais pode haver a necessidade de as repetir

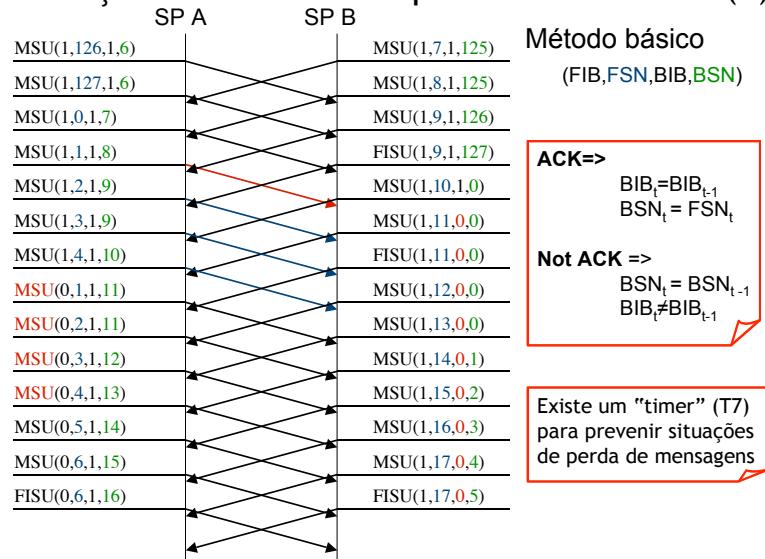
Correcção de erros: exemplo método básico



Correcção de erros: exemplo método básico (2)



Correcção de erros: exemplo método básico (3)



Funções do MTP nível 2: Alinhamento inicial

- **Objetivo:** Sincronização ao nível das Unidades de Sinalização utilizando LSSUs que vão indicando o estado da ligação. Confirmação da taxa de erros na ligação.
 - Aplicável na activação e restauração de uma ligação.
 - É executado independentemente em cada "link".
 - Existem dois períodos de prova:
 - Normal (2^{16} Tempo de transmissão de 1 octeto)
 - Emergência (2^{12} Tempo de transmissão de 1 octeto)
 - Decisão tomada pelo nível 3 unilateralmente num dos extremos da ligação (invocação da primitiva **start**). Se não houver link activo entre dois SP o nível 3 opta pelo alinhamento de emergência.
 - Estados possíveis:
 - **SIOS:** *Status Indication Out of Service* - depois de "power up" FSN=BSN=127, FIB=BIB=1 (LSSU enviadas até o nível 3 invocar a primitiva "start").
 - **SIO:** *Status Indication Out of Alignment* - o alinhamento ainda não foi adquirido.
 - **SIN:** *Status Indication Normal Alignment* - caso normal existe outro "link" em funcionamento.
 - **SIE:** *Status Indication Emergency Alignment* - não existe nenhum link entre os dois SP
 - **SIPO:** *Status Indication Processor Outage* - serve para indicar o outro extremo que as mensagens não podem ser entregues pelo nível 2 ao nível 3.

Funções MTP2: Monitorização da taxa de erros

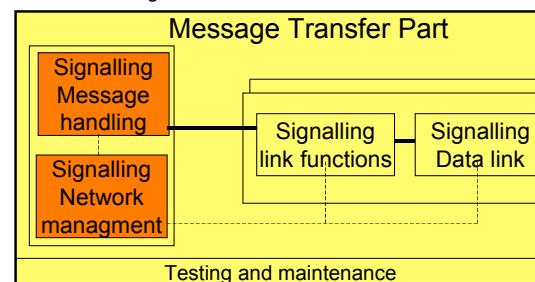
- Monitorização da taxa de erros é efectuada em duas fases:
 - Na fase de alinhamento da ligação (*Alignment error rate monitor - AERM*) em que:
 - Incrementa um contador por cada LSSU recebida com erro (ou incrementa o contador por cada N (N=16) bytes recebidos se no modo de contagem de octetos.)
 - O período de prova é abortado e o contador excede um valor fixado. ($T_{normal} = 4$, $T_{emergencia} = 1$). Reinicia-se novo período de prova, (em emergência aceita uma taxa de erros de 10^{-4}).
 - Ao fim de M ($M=5$) tentativas a ligação é posta fora de serviço.
 - Com a ligação em serviço (*Signal unit error rate monitor - SUERM*), em que a taxa de erros medida com base no princípio do *token bucket*:
 - Por cada SU errada um contador é incrementado (No modo contagem de octetos o contador é incrementado por cada octeto lido)
 - O contador é decrementado de 1 por cada bloco de D SUs consecutivos correctas (não decrementa se contador = 0)
 - Caso o contador atinja um valor T o link é posto fora de serviço (se se verificar uma taxa de erros excessiva, $>4 \times 10^{-3}$).
 - (Nota para links de sinalização de 64kbps temos $D=256$ e $T=64$)

Funções MTP2: Controlo de Fluxo

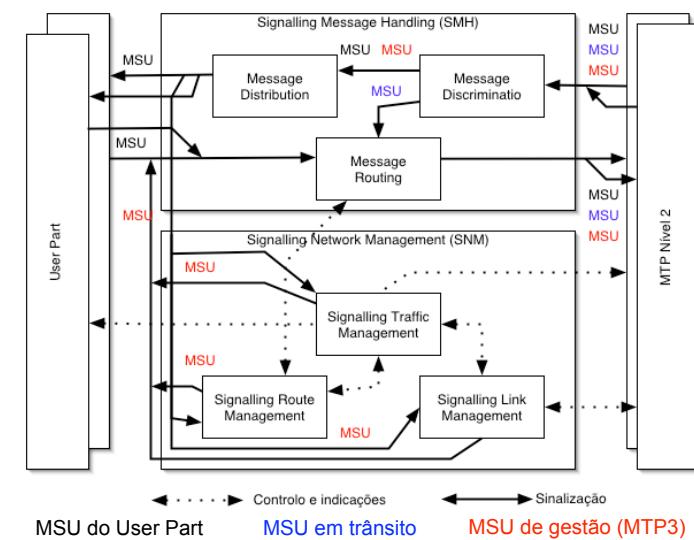
- O Processo detecção de congestão é dependente da aplicação.
- Quando é detectada congestão é enviado para o outro extremo uma LSSU com indicação de "SIB" -Status Indication Busy.
 - Ao mesmo tempo são retidos todos os ACKs das mensagens recebidas.
 - Periodicamente é reenviado "SIB" até que termine a condição (T_5 - 80 a 120 milisegundos).
 - Na recepção de um LSSU com indicação de congestão, deixa de enviar mais mensagens.
- Se o tempo de ocorrência de congestão for demasiado longo a ligação é posta fora de serviço para o nível 3 (3 a 6 segundos.)
- Numa situação de congestão a transmissão pode continuar no outro sentido.

Funções MTP nível 3: Funções de Rede

- Define um conjunto de funções comuns e independentes do funcionamento de cada ligação individual.
- São executadas em cada SP (e STP).
- Contém um vasto leque de funções e opções. O conjunto a aplicar depende da estrutura e exigências da rede.
- Existem dois grupos de funções:
 - Tratamento de mensagens de sinalização: actuam na fase de transferência da mensagem para determinar qual a ligação de sinalização a utilizar ou qual o utilizador a quem entregar a mensagem (encaminhamento - comutação).
 - Gestão da rede de sinalização: controlam os encaminhamentos e a configuração da rede baseado no seu estado. Tenta assegurar a manutenção das capacidades normais de transferência de mensagens em caso de falha na rede.

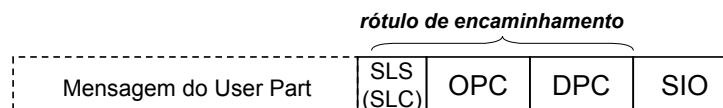


MTP nível 3: Arquitectura



MTP nível 3: Tratamento das mensagens (Signalling Message Handling)

- **Discriminação (Discrimination):** é efectuada com base no DPC e determina se a mensagem é entregue a um utilizador (*User Part*) nesse nó ou se a mensagem é transferida para outro nó.
 - **Distribuição (Distribution):** Com base no SIO determina qual o utilizador (UP) a que deve ser entregue a mensagem. Se não for possível fazer a entrega é devolvida uma indicação ao utilizador originante para que este reduza o tráfego com aquele destino.
 - **Encaminhamento (Routing):** É realizado de uma forma independente em cada nó. É baseado em:
 - Rótulo de encaminhamento: determina a origem (*OPC*) o destino (*DPC*) e a ligação a usar (*SLS - Signalling Link Selection*, ou *SLC - SL Code*);



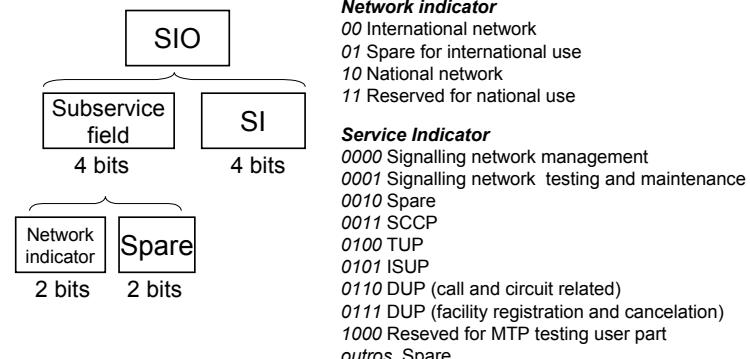
- Tabelas de encaminhamento actualizadas em função dos acontecimentos na rede. Para cada destino é definido um conjunto de rotas alternativas a utilizar em caso de falha.

MTP nível 3: Partilha de Carga, selecção de *links*

- A partilha de carga tem por função distribuir o tráfego pelas ligações de sinalização disponíveis para um dado destino.
 - Vantagens:
 - Minimizar os efeitos de falhas
 - Maior capacidade para suportar picos de tráfego
 - É efectuado com base no campo SLS do rótulo, todas as mensagens com o mesmo SLS utilizam a mesma ligação de sinalização (*signalling link*).
 - A função é comandada pelo utilizador (UP) que gera a mensagem. O UP é o responsável por garantir a sequencialidade para uma dada transacção. Excepto em casos de falha na MTP.
 - As mensagens do nível MTP 3 são um caso especial pois o SLC (e não SLS) depende do tipo da mensagem podendo indicar qual a ligação de sinalização a que se refere (o SLS respectivo) e não a que deve ser utilizada para o seu transporte.

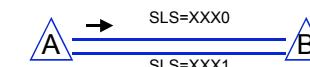
MTP nível 3: Tratamento das mensagens (Signalling Message Handling)

- ... pode ainda analisar o Service Information Octet (SIO), composto por:
 - *Service Indicator*, permite encaminhamentos diferentes para cada utilizador
 - *Network Indicator*, permite distinguir qual a estrutura de numeração do Point code a utilizar e qual a estrutura de rótulo de encaminhamento.

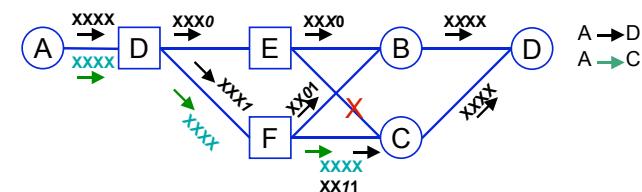


MTP nível 3: Exemplos de partilha de carga

- Entre ligações do mesmo “link set” (única situação possível no modo associado):



- Entre ligações de “link set” distintos:
 - Corresponde a utilizar rotas diferentes
 - Exige que existam STP(s) na rota
 - Normalmente só utilizado quando não existem ligações directas ao SP destino
 - Dentro de cada “link set” pode depois ser aplicado o método anterior

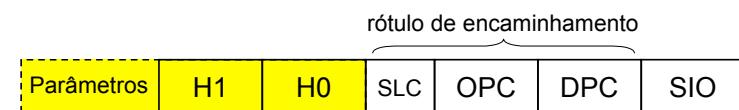


MTP nível 3: Gestão da rede de Sinalização

- As duas principais funções da gestão da rede de sinalização são:
 - A **reconfiguração no caso de falhas**, as falhas podem ocorrer nos SP, nos STP, nas ligações. Em caso de falhas o tráfego será desviado para caminhos alternativos.
 - A **gestão de tráfego durante as situações de congestão**. Quando ocorre congestão em parte duma rede de sinalização o tráfego terá que ser reduzido até que a congestão desapareça.
- São três as funções genéricas para lidar com estas situações:
 - Signalling link management**, gestão das ligações de sinalização, responsável por gerir as ligações locais e tenta manter o número normal de ligações em serviço num "link set".
 - Signalling traffic management**, gestão do tráfego de sinalização, responsável pelo encaminhamento de acordo com o estado da rede e pelo controlo de fluxo.
 - Signalling route management**, gestão das rotas de sinalização, só aplicável no modo quase-associado e é responsável pela transferência entre os pontos de sinalização de informação relativa ao estado das rotas de sinalização.

MTP nível 3: Formato das mensagens de gestão

- Service Information, SI=0000
- Signalling Link Code - SLC:** identificação do link a que a mensagem de gestão diz respeito. (Caso a mensagem não se refira a nenhum *link* em particular SLC=0.)
- Headers H0, H1:** H0 indica o grupo de funcionalidades a que a mensagem pertence (e.g., *Changeback*), H1 indica uma mensagem em particular dentro do grupo (e.g., *Changeback ack.*)



MTP nível 3: Gestão das ligações de sinalização: *Signalling Link Management (SLM)*

- Estado das ligações de sinalização:
 - Disponível**, pode transportar mensagens geradas nos níveis 3 e 4.
 - Indisponível**, não pode transportar mensagens de sinalização (Com exceção, no caso de inibição, de mensagens de teste do nível 3.)
- Critérios de indisponibilidade:
 - Ligaçāo inactiva**, não existe comunicação com o nível 2 ou não há associação entre um "signalling data link" e um "signalling terminal".
 - Ligaçāo com falha**, por indicação do nível 2 causada por:
 - Excesso de erros
 - Excessivo período de alinhamento
 - Excessivo período de congestão
 - Ligaçāo bloqueada**, existe uma condição de "Processor Outage" no terminal remoto.
 - Ligaçāo inibida**, por pedido explícito do sistema de gestão em qualquer dos extremos da ligação para efeitos de teste e manutenção, não havendo alteração de estado de nível 2 mas a ligação fica indisponível para transporte de tráfego dos UP's. Só pode transportar mensagens de nível 3 de teste e manutenção. Não pode causar inacessibilidade de nenhum destino.

MTP3 (SLM): Atribuição de um "signalling data link" e de "signalling terminals" a um "signalling link".

- Antes de activar um "signalling link" é necessário atribuir um "signalling data link" e um "signalling terminal" em cada extremo. (Um MTP3 pode escolher entre diferentes *signalling data links*, ex. diferentes *time slots*.)
- Estão definidos 3 conjuntos de procedimentos de acordo com o nível de automatização implementado:
 - Basic signalling link management**: A atribuição de "signalling data link" e de "signalling terminal" é feita manualmente.
 - Automatic allocation of signalling terminals only**: um terminal de sinalização é escolhido entre os disponíveis. A atribuição de um "signalling data link" é manual.
 - Automatic allocation of signalling data link and signalling terminals**: um terminal de sinalização é escolhido entre os disponíveis. O mesmo "signalling data link" tem que ser atribuído nos dois extremos.

MTP3 (SLM): Procedimentos Básicos de Gestão de Ligação

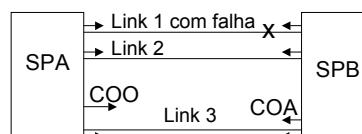
- **Activação**, ligação entre o Signalling Data Link e o respectivo terminal de sinalização. Execução do procedimento de alinhamento inicial (nível 2). Execução de um teste para verificação que a ligação termina no destino pretendido.
- **Restauro**, é executado após ser detectada uma falha na ligação. Consiste na execução do procedimento de alinhamento inicial (nível 2) e execução de um teste para verificação que a ligação termina no destino pretendido.
- **Desactivação**, o terminal é desligado do Signalling Data Link, só pode ser executado se a ligação não transportar tráfego nesse momento.
- **Activação de um conjunto de ligações**, executado quando um conjunto de ligações não tem nenhuma ligação em serviço. Consiste na activação do maior número possível de ligações desse conjunto. O tráfego pode iniciar-se logo após a primeira ligação ter sido activada com sucesso.

MTP3: Relação com o *Signalling route management*

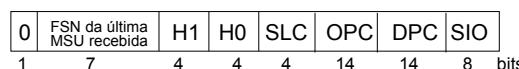
- O estado das rotas de sinalização é determinado por um dos STPs nessa rota que informa os nós adjacentes desse estado. O estado pode ser:
 - Disponível
 - Indisponível
- Estado das pontos de sinalização:
 - Disponível - quando pelo menos uma ligação local está disponível
 - Indisponível- quando todas as ligações estão indisponíveis.
- Nota: cada ligação, rota ou ponto de sinalização disponível pode também ser considerada como em congestão ou não.

Funções MTP nível 3: Gestão da Rede Procedimentos de gestão de tráfego

- Procedimento de *Changeover*,
 - Tem como objectivo o desvio, para uma ligação alternativa, do tráfego transportado por uma ligação que ficou indisponível, assegurando tanto quanto possível a manutenção a sequência das mensagens. O tráfego pode ser desviado para uma ou mais ligações alternativas. As ligações alternativas são:
 - As restantes ligações disponíveis no "link set"
 - Uma ou várias ligações dum "link set" alternativo (se não existir o anterior). É determinado de acordo com as rotas alternativas definidas para cada destino.
 - O tráfego já existente nas ligações alternativas não é interrompido.
 - Antes do desvio do tráfego é efectuado um procedimento para determinar o ponto a partir do qual deve ser reiniciada a transmissão das mensagens (o FSN da última MSU).
 - Mensagens trocadas: Changeover order signal (COO) / acknowledge (COA)

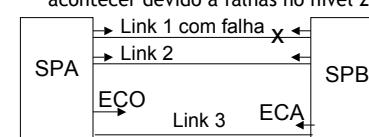


SIO, Campo SI=0000
SLC, indicação do link em falha (Link 1)
H0=0001, Changeover
H1=(0001,COO) ou (0010, COA)
Parâmetros = FSN da última MSN recebida



Funções MTP nível 3: Gestão da Rede Procedimentos de gestão de tráfego

- Procedimento *Emergency Changeover*,
 - Tem os mesmos objectivos que o anterior mas aplica-se quando não for possível obter o FSN da última mensagem recebida correctamente. (isto pode acontecer devido a falhas no nível 2 desse SP).
- Procedimento *Time-Controlled Changeover*,
 - É aplicado quando não se pode ou não é aconselhável trocar as mensagens usuais do Changeover (COO,COA). (isto pode acontecer quando um "link" for colocado em "inhibit", em que não se deve perder mensagens quando se desvia o tráfego para uma rota alternativa.). O SP desvia o tráfego ao fim de T1 segundos.
- Procedimento de *Changeback*
 - Procedimento oposto ao *Changeover*,
 - Tem como objectivo o restaurar o mais rapidamente possível o fluxo de tráfego para a sua ligação normal. É executado quando a ligação normal para um determinado tráfego deixa de estar indisponível. Pode provocar perda de sequência das mensagens.

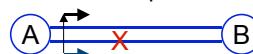


SIO, Campo SI=0000
SLC, indicação do link em falha (Link 1)
H0=0010, Emergency Changeover
H1=(0001,ECO) ou (0010, ECA)
Parâmetros = FSN da última MSN recebida

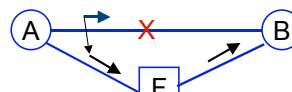
Funções MTP nível 3: Gestão da Rede

Exemplos de desvios de tráfego

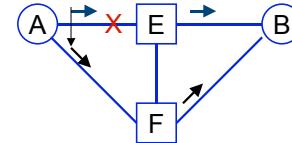
- Passagem para um canal alternativo paralelo.



- Passagem para um canal de socorro pertencente a um caminho de sinalização passando por um ponto de sinalização remoto.



- Passagem para um canal de socorro que não passa pelo mesmo ponto de sinalização remoto.

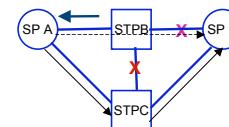


Funções MTP nível 3: Gestão da Rede

Procedimentos de gestão de tráfego

- Procedimento de *Forced Rerouting*,

- Tem como objectivo restaurar o mais rapidamente possível a capacidade de sinalização para um destino cuja rota ficou inacessível sendo o tráfego desviado para uma rota alternativa.
É executado quando se recebe uma mensagem indicando que o destino em causa ficou inacessível para um STP desta rota (*Transfer Prohibited*). Distingue-se do *changeover* porque a falha não é detectada localmente e só afecta o tráfego para o destino em causa.
Existe uma alta probabilidade de perda de sequência das mensagens, a estrutura da rede pode diminuir esta probabilidade. Só é aplicado no modo quase-associado.



1. A rota A-B-C está inacessível.
O STP B avisa SP A que a rota que estava a ser utilizada para SP D está inacessível.
2. Necessidade de desviar o tráfego
Usar A-B-C-D (seria um changeover)
Solução: A-C-D

- Controlled Rerouting,

- Tem como objectivo restaurar o encaminhamento normal das mensagens para um determinado destino minimizando a possibilidade de perda de sequencialidade.
Procedimento oposto ao *Forced Rerouting*. É executado quando é recebida uma mensagem indicando o retorno ao estado de disponibilidade de uma rota (*Transfer Allowed*).
Só é aplicado no modo quase-associado.

Funções MTP nível 3: Gestão da Rede

Procedimentos de gestão de tráfego

- Management Inhibiting

- Tem como objectivo tornar uma ligação indisponível para o transporte de tráfego gerado pelo nível 4.
É executado a pedido do sistema de gestão do nó para que possam ser efectuadas operações de manutenção e teste na ligação.
Não causa mudança de estado no nível 2.
- O pedido não é executado se causar a inacessibilidade de algum destino ou for causa de congestão.
- A ligação mantém-se inibida até que o sistema de gestão faça um pedido de desinibição ou se for necessário restaurar a acessibilidade de um destino.
- Se a ligação transportar tráfego este pedido causa o desvio do tráfego para ligações alternativas através do procedimento de *changeover*.

Mensagem, valores de H0, H1

H1=0001, LIN- Link Inhibit Signal
H1=0010, LUN- Link Uninhibit Signal
H1=0011, LIA- Link Inhibit Acknowledgment Signal
H1=0100, LUA- Link Uninhibit Acknowledgment Signal
H1=0101, LID- Link Inhibit Deneid Signal
H1=0110, LFU- Link Forced Uninhibit Signal
H1=0111, LLT- Link Local Inhibit Test Signal
H1=1000, LRT- Link Remote Inhibit Test Signal

H0 = 0110

Funções MTP nível 3: Gestão da Rede

Procedimentos de gestão de tráfego

- MTP restart*

- Um SP ou STP está completamente isolado da rede quando todos os "links" para nós adjacentes não estão disponíveis.
- MTP Restart tenta trazer de novo o SP ou STP à rede através da restauração do tráfego com os nó adjacentes.
- Durante uma situação de isolamento de um SP ou STP ele não recebe mensagens de "Transfer prohibited ou restrict" pelo que as suas tabelas de encaminhamento não estão actualizadas. É muito importante a troca de informação para actualização das tabelas e que o procedimento seja breve para evitar alterações de estado durante o mesmo.
- Para actualizar as tabelas os nós adjacentes enviam dois tipos de mensagens ao SP que executa o MTP restart:
 - TRP- Transfer prohibited (ou TFR Transfer restricted opção nacional)
 - TRA- Traffic restart Allowed

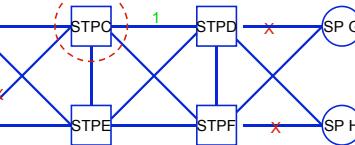
Mensagem, valores de H0, H1

H0 = 1000, H1= 0001

Funções MTP nível 3: Gestão da Rede

Procedimentos de gestão de tráfego

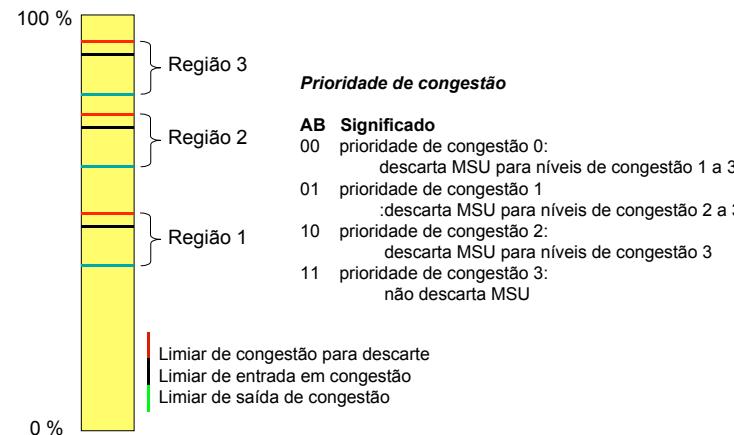
- **Exemplo MTP restart**
 1. O nó C encontra-se isolado
 2. Entretanto falham as ligações:
 1. G-D, H-F e B-C.
 3. Se a ligação C-D fica boa
 4. O Nó STP D envia TFP e TFR para o STP C.
 5. Depois envia TRA para o STP C.
 6. A primitiva MTP-RESUME é então enviada para os utilizadores
 7. Se o caminho D-E-C ficar disponível, mensagens TFP e TFR são enviadas para o STP C por este caminho



Funções MTP nível 3: Gestão da Rede

Procedimentos de gestão de tráfego

- Controlo de Fluxo: Exemplo de um *buffer* com 4 níveis



Funções MTP nível 3: Gestão da Rede

Procedimentos de gestão de tráfego

- **Controlo de Fluxo (Flow Control)**
 - Tem como objectivo limitar o fluxo de tráfego na fonte quando a rede não pode transportar todo o tráfego oferecido.
 - É executado devido a uma falha na rede que provocou a inacessibilidade de um nó, congestão numa ligação ou nó, ou falha num utilizador que impede a entrega das mensagens recebidas pelo MT, só afecta o tráfego referente a este utilizador.
 - Quando as condições cessam é restabelecido o fluxo normal.
 - Signalling link Congestion, é medida pela ocupação dos buffers do nível 2. Existe um limiar de congestão acima do qual se considera o "link" congestionado e um limiar abaixo do qual se considera que terminou aquela situação. Os limiares são distintos para evitar oscilações.
 - Na rede internacional o link ou é considerado em congestão ou não.
 - Na rede nacional podem-se definir até 4 estados de congestão, um não congestionado e três referentes a 3 níveis diferentes de congestão.
 - Se se definirem prioridades para as MSUs pode-se ter uma rede de sinalização nacional usando múltiplos estados de congestão. Este último é usado nos EUA

Funções MTP nível 3: Gestão da Rede

Tratamento da congestão (internacional)

- A congestão de uma ligação é detectada pelo nível 2 com base no nível de MSUs nos buffers de transmissão e retransmissão.
- A deteção da congestão de um nó é dependente da implementação.
- A MTP não limita o tráfego enviado pelos utilizadores. Apenas lhes indica essa necessidade.
- A MTP não despreza mensagens a não ser em casos extremos de falta de recursos.
- Um conjunto de rotas é considerado congestionado se, pelo menos uma das ligações desse conjunto estiver congestionado, ou for recebida essa indicação de um STP adjacente.
- No caso de um utilizador enviar uma mensagem para um conjunto de rotas congestionado a mensagem é passada ao nível 2 para transmissão e o utilizador é informado da situação de congestão.
- O fim do estado de congestão é detectado pelos utilizadores quando ao enviar uma mensagem não recebem indicação de congestão .

Funções MTP nível 3: Gestão da Rede Gestão de rotas

- Assegura que todos os nós tem informação actualizada sobre o estado das rotas de sinalização. Modo quasi-associado:
 - *Transfer prohibited* -Transferência proibida, objectivo: Informar os nós adjacentes que uma dada rota ficou indisponível. Executada só em nós com funções STP, quando um STP detecta que um destino ficou inacessível envia uma indicação para todos os nós adjacentes, ou quando um STP recebe uma mensagem para um desti-no inacessível envia a indicação para o nó de onde a mensagem foi recebida. O nó adjacente que recebe esta mensagem executa um "forced rerouting", se não for possível executa por sua vez este procedimento.
 - *Transfer allowed*, Transferência permitida, objectivo: Informar os nós adjacentes que uma dada rota retorna ao estado disponível. Executada só em nós com funções STP, quando um STP detecta os nós adjacentes podem cursar tráfego através dele. Pode desencadear "Controlled Rerouting" nos nós adjacentes.
 - *Transfer restricted* Transferência controlada, objectivo: propagar a indicação de congestão desde o SP que detectou congestão até ao originante. Enviado por um STP para um nó adjacente quando recebe deste uma mensagem para uma rota congestionada.

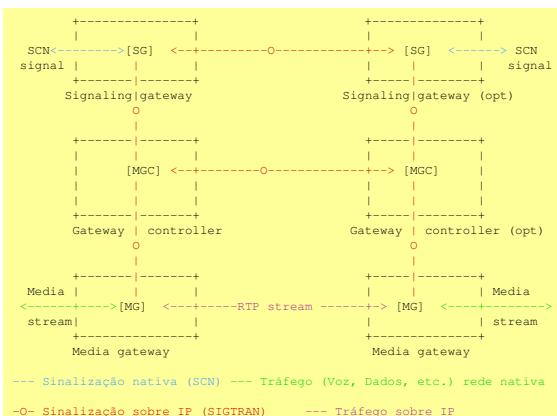
Funções MTP nível 3: Gestão da Rede Gestão de rotas

- *Signaling Route Set Test*, é a função utilizada quando um SP recebe dum STP adjacente a mensagem "transfer prohibited" ou a mensagem "transfer restricted" para um destino particular. A finalidade deste teste é detectar quando termina a condição que desencadeou aquelas mensagens. É enviada a mensagem " route set test" priodicamente (30 a 60 s) do SP para o STP. Quando o SP recebe "Transfer allowed" termina o envio de "route set test".
- *Signaling Route Set Congestion*. Em cada SP existe um estado de congestão associado a cada ligação ("link"). Considera-se que um caminho para um dado destino se encontra congestionado se pelo menos um "link" do caminho para esse destino ficar congestionado. Dois procedimentos podem actualizar o estado de congestão dum caminho:
 - "Transfer controlled procedure" só para redes que não utilizem múltiplos níveis de congestão) e utiliza a mensagem "Transfer controlled" enviada pelo STP para o SP que ao recebe-la reduz o tráfego para o SP mencionado. O STP reenvia esta mensagem a cada 8 mensagens enquanto dure a situação.
 - "Signaling Route Set Congestion procedure" utiliza a mensagem "Route Set Congestion test". Enviada pelo SP que reduziu o tráfego para o SP destino para pedir uma actualização do estado de congestão

Transporte de Signalização sobre IP (SIGTRAN)

- O SIGTRAN é:
 - Um grupo da IETF dedicado ao estudo do transporte de informação de sinalização (por mensagens) sobre redes IP.
 - <http://www.ietf.org/html.charters/sigtran-charter.html>
 - Exemplos de aplicação:
 - Controlo de acesso à Internet por *dial-up*
 - Interligação de telefonia sobre IP com a PSTN (PLMN, ISDN)
 - Acesso a entidades do SCN a bases de dados (na Internet)
 - Desenvolvimento de novos serviços
 - Conjunto de drafts e RFCs (alguns exemplos):
 - Architectural Framework for Signaling Transport (RFC 2719)
 - Stream Control Transmission Protocol (RFC 2960)
 - SCTP Protocol Management Information Base (RFC 3873)
 - ISDN Q.921-User Adaptation Layer (RFC 3057)
 - Signalling Connection Control Part User Adaptation Layer (SUA) (RFC 3868)
 - SS7-MTP2: User Peer-to-Peer Adaptation Layer (M2PA) (RFC 4165)
 - SS7-MTP3: User Adaptation Layer (M3UA) (RFC 4666)

Entidades lógicas da arquitectura

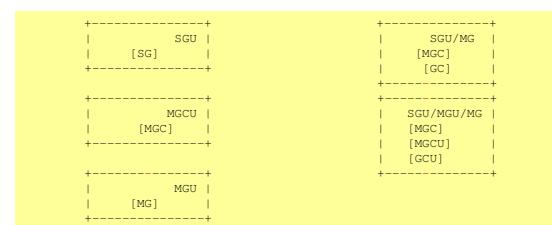


- **Nota:**
 - Esta arquitectura é genérica e independente da SCN

Arquitectura Genérica para Transporte de Signalização sobre IP

- Âmbito de uma arquitectura para transporte de sinalização:
 - Definição de métodos de encapsulamento (formato)
 - Protocolos extremo-a-extremo
 - Suporte, utilizando as capacidades do IP, dos requisitos funcionais e não-funcionais do transporte de sinalização
 - Arquitectura Genérica:
 - Define entidades funcionais e físicas
 - Definição de relações entre entidades funcionais (físicas)
 - Definição de requisitos para o transporte de sinalização
 - Alguns termos importantes:
 - *SCN: Switched Circuit Network*
 - Rede que transporta o tráfego (e.g., PSTNs, PLMNs)
 - *SEP: Signaling End Point*
 - *STP: Signaling Transfer Point*
 - *Backhaul*
 - *Transporte de sinalização desde a interface onde é recebida a informação de sinalização até ao ponto onde essa informação é processada*

Entidades físicas da arquitectura



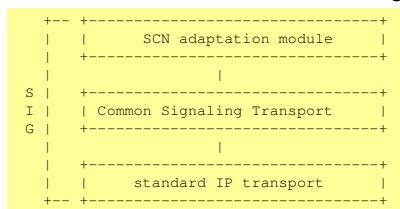
- O que não faz parte da arquitectura:**

 - *Definição do protocolo de sinalização*
 - *Especificação das funções dentro do SGU e MGU*
 - *Algumas das funções de gestão do SGU e MGU*
 - (e.g., determinação de IPs, teste das ligações)

Componentes

- *Media Gateway Unit*
Unidade física contendo a funcionalidade MG
 - *Media Gateway Controller Unit*
Unidade física contendo a funcionalidade MGC
 - *Signaling Gateway Unit*
Unidade física contendo a funcionalidade SG
 - (Entidades em que são implantadas várias funcionalidades)

Arquitectura protocolar *Signaling Transport(SIG)*



Componentes Arquitectura Protolocalar SIC

SCN adaptation module

- Suporte das primitivas específicas do protocolo de sinalização

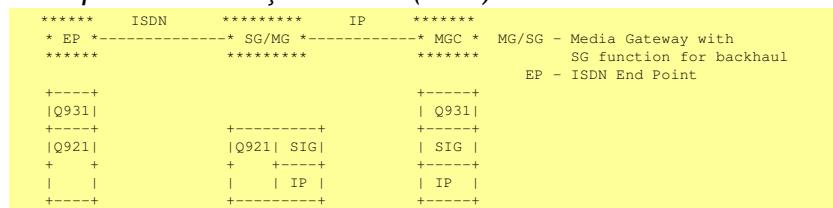
Common Signaling Transport

 - Conjunto de funcionalidades para o suporte de protocolos de sinalização

standard IP transport

 - Protocolo IP não-modificado

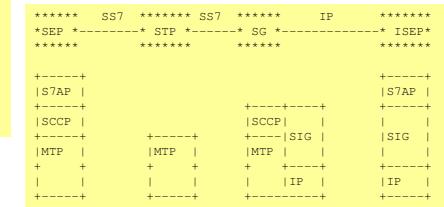
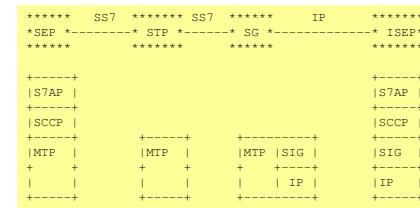
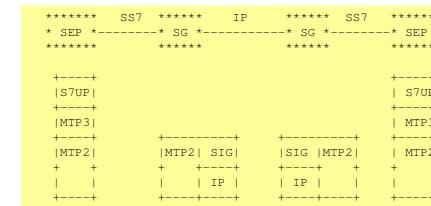
Exemplo de utilização do SIG (RDIS)



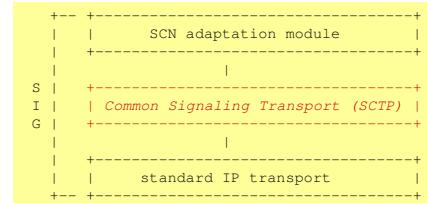
Requisitos Signalização sobre IP

- Requisitos Funcionais Genéricos
 - Suporte e identificação para diferentes tipos de protocolos de sinalização
 - Definição de um protocolo base comum para o transporte de sinalização
 - Disponibilizar as funcionalidades definidas para os níveis inferiores do SCN
 - Ex.: Controlo de fluxo, ordenamento de msgs, detecção de erros
 - Multiplexagem de várias sessões SCN na mesma sessão de transporte
 - Controlo de congestão (podendo utilizar funções do SCN)
 - Requisitos de Desempenho para SS7 (exemplos):
 - Perda de mensagens: < 1 em $1E+7$
 - Mensagens fora de sequência: <1 em $1E+10$
 - Mensagens com erro (não detectado pelo transporte): <1 em $1E+9$
 - Disponibilidade: < 10 min por ano fora de serviço
 - Procedimentos extremo-a-extremo: atraso < 500 a 1200ms

Signalling Transport (SIG) e SS7



Implementação da arquitectura: SCTP (*Stream Control Transmission Protocol*)

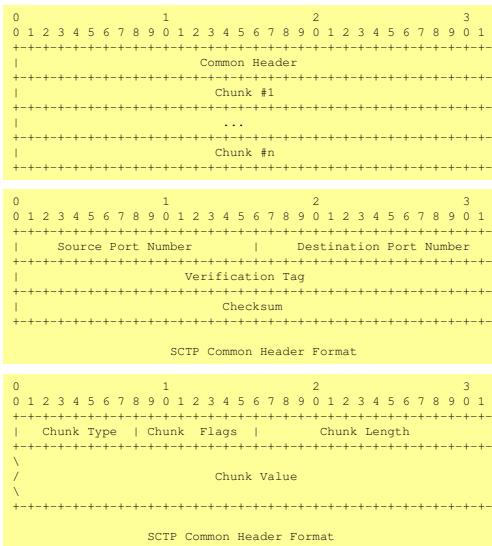


Interface para o nível superior:

- **Inicialização do SCTP**
 - `INITIALIZE ([local_port])`
 - **Inicialização de uma associação**
 - `ASSOCIATE(local, remote, ...)`
 - **Terminação de uma associação**
 - `SHUTDOWN(association_id)`
 - **Envio de mensagem**
 - `SEND(assoc_id, buffer, count, ...)`
 - **Recepção de mensagem**
 - `RECEIVE(assoc_id, buffer, size, ...)`
 - **Pedido de heartbeat**
 - `REQUESTHEARTBEAT(assoc_id, dest_addr)`

- *O SCTP é um protocolo fiável de nível transporte sobre uma rede não fiável e sem ligação (IP)*
 - *Oferece os seguintes serviços:*
 - *Trânsferencia de dados confirmada, ordenada e sem duplicados*
 - *Utilização de um TSN para as mensagens*
 - *Disponibilidade verificada com “heartbeats”*
 - *Multiplexagem de várias msg num mesmo pacote SCTP (ordenamento por fluxo de msgs)*
 - *Controlo de fluxo*
 - *Mecanismos de segurança (baseados em cookies)*

Implementação da arquitectura: SCTP (Formato das mensagens)



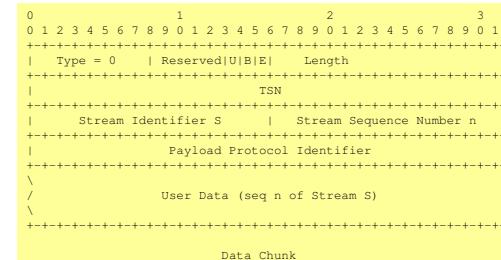
- **IP + Porto**
identifica cada extremo do SCTP

- **Verification Tag**
Utilizado para verificar a origem da mensagem

- **Chunk Type**

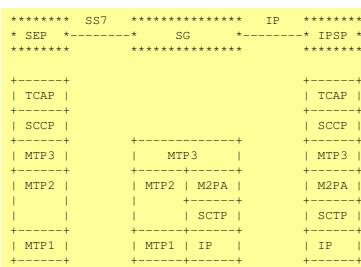
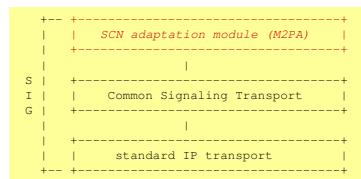
- 0 - Payload Data (DATA)
- 1 - Initiation (INIT)
- 2 - Initiation Ack (INIT ACK)
- 3 - Selective Ack (SACK)
- 4 - Heartbeat Request (HEARTBEAT)
- 5 - Heartbeat Ack (HEARTBEAT ACK)
- 6 - Abort (ABORT)
- 7 - Shutdown (SHUTDOWN)
- 8 - Shutdown Ack (SHUTDOWN ACK)
- 9 - Operation Error (ERROR)
- 10 - State Cookie (COOKIE ECHO)
- 11 - Cookie Ack (COOKIE ACK)
- 12 - ...

Implementação da arquitectura: SCTP (Formato das mensagens)



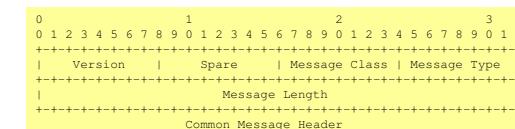
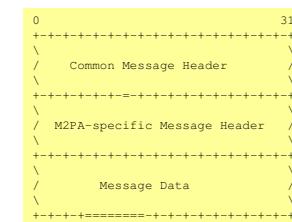
- **(U) nordered chunk**
- **(B)egining fragment bit**
- **(E)nding fragment**
- **(T)ransmission (S)eq. (N)umber**
- **(S)tream Identifier**
- **Stream Sequence (N)umber**
 - Numeração dentro do fluxo
- **Payload Protocol Identifier**
 - Identifica o utilizador (protocolo)
 - Não utilizado pelo SCTP

Implementação da arquitectura: M2PA (MTP2 - User Peer-to-Peer Adaptation Layer)



- O M2PA disponibiliza ao MPT3 uma interface e serviços idênticos aos do MTP2
 - Todos os serviços da interface MPT3/MPT2
- Utiliza os serviços do STCP.
 - Uma associação STCP representa um link SS7
- Comunicação peer-peer MPT2
 - MSU = User Data
 - LSSU = Link Status
 - FISU (não existem no M2PA)
 - MSUs são confirmadas através de mensagens User Data vazias
- Funcionalidades disponibilizadas
 - Recuperação de dados (MTP3 changeover)
 - Reporting Link Status ao MPT3
 - Procedimento de Processor Outage
 - Procedimento de Link Alignment

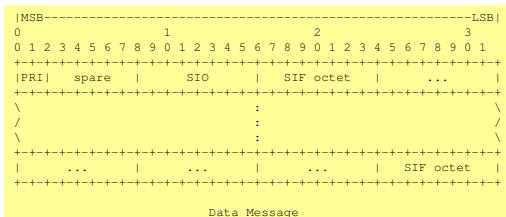
Protocolo M2PA: Formato das mensagens



- **Common Msg Header**
 - Version: MP2A 1.0 (1)
 - Message Class: M2PA (11)
 - Message Type
 - User Data (1)
 - Link Status (2)

- **M2PA-specific Header**
 - FSN: Forward Seq.
 - BSN Backward Seq

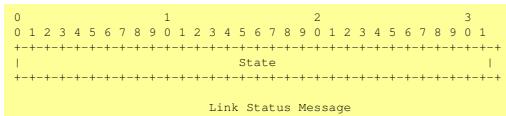
Protocolo M2PA: Formato das mensagens



- *Data Message*

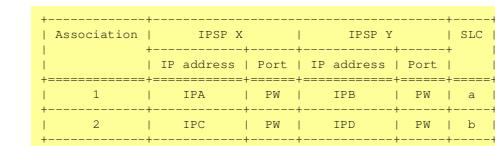
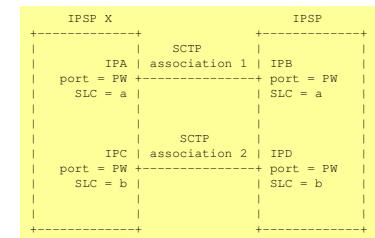
- *PRI*: Priority
- *SO*: Service Info Octet
- *SIF*: Signaling Info Field
- **Não contém:**
 - Flag,
 - BSN, FSN, BIB, FIB
 - Length Indicator (LI)
 - Check Bits (CK)

- *Link Status Message*



- 1 Alignment
- 2 Proving Normal
- 3 Proving Emergency
- 4 Ready
- 5 Processor Outage
- 6 Processor Recovered
- 7 Busy
- 8 Busy End
- 9 Out of Service (OOS)

Protocolo M2PA: Entidades MTP e STCP



O projecto OpenSS7

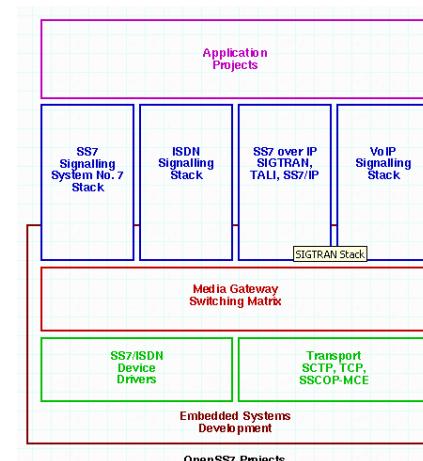
- O projecto OpenSS7 é:

- Biblioteca de fonte aberta (*opensource*) implementando a pilha protocolar do SS7 e SIGTRAN para Linux.
- Encontra-se disponível em <http://www.openss7.org>

- Motivação para o projecto OpenSS7:

- Contribuir para uma utilização mais vasta do SS7, através de:
 - Uma solução de baixo custo (código disponibilizado, licença GPL).
 - Implementação simples da pilha SS7 e de fácil integração
 - Baseada em arquitecturas e interfaces abertas (e.g., STREAMS)
 - Promoção da colaboração no desenvolvimento/certificação Sw.

Arquitectura do OpenSS7



- Conjunto de módulos independentes do transporte
- Utilização de OSI STREAMS
 - Conjunto de primitivas comuns (utilizadas em todas as interfaces)
- Pilhas protocolares para SS7:
 - Pilha protocolar SS7
 - **SS7 sobre IP (SIGTRAN)**



Instituto Universitário de Lisboa
Lisbon University Institute

IMS
IP Multimedia Subsystem

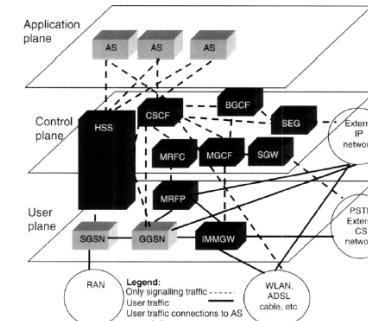
O IP Multimedia Subsystem (IMS)

- “O IMS é um sistema global, independente do sistema de acesso, baseado em normas, com connectividade IP e arquitecturas de controlo de serviços que permite disponibilizar diferentes tipos de serviços multimedia a utilizadores finais utilizando protocolos comuns da Internet”.

A arquitectura IMS

Baseada em planos:

- Plano das aplicações: onde está a lógica dos serviços
- Plano de controlo: controlo das chamadas, recursos
- Plano do utilizador/transporte: interligação com os terminais (rede de acesso)



A arquitectura IMS: P-CSCF

Elementos da arquitectura:

- Gestão de sessões e encaminhamento:
 - Call Session Control Function (CSCF)*

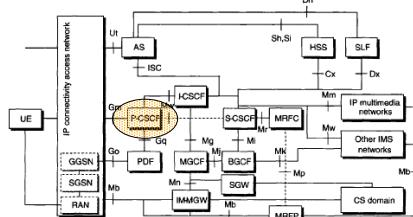
Envolvidos no processo de registo de terminais e estabelecimento de sessões.

Existem três variantes do CSCF:

Proxy Call Session Control Function (P-CSCF): primeiro ponto de contacto do equipamento dos utilizadores (UE) com a rede IMS (quer O quer T).

Responsável por manter a integridade e segurança com o UE.

Interage com o *Policy Decision Function (PDF)* por forma a determinar parâmetros de QoS e interagir com os sistemas de taxação.



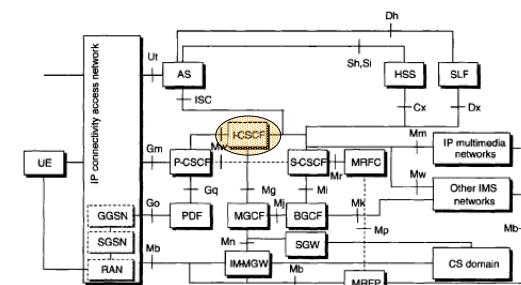
A arquitectura IMS: I-CSCF

Elementos da arquitectura:

- Gestão de sessões e encaminhamento:

Interrogating Call Session Control Function (I-CSCF): ponto de contacto com a rede origem (*home network*).

- Atribuir um S-CSCF baseado na descrição de capacidades fornecida pelo HSS.
- Obter da base de dados HSS o próximo salto (S-CSCF ou AS) para a informação de sinalização.



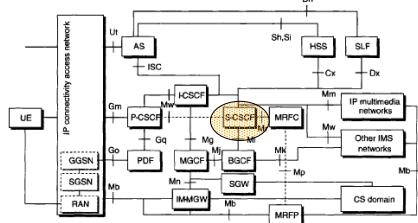
A arquitetura IMS: S-CSCF

Elementos da arquitectura:

- Gestão de sessões e encaminhamento:

Serving Call Session Control Function (S-CSCF): elemento central da arquitectura IMS - toda a informação de e para o UE passa por um S-CSCF, são responsáveis por:

- Processo de registo.
 - Processo de encaminhamento da sinalização e manutenção do estado das sessões (e.g., para uma rede diferente, IMS ou não).
 - Registo do perfil de serviços (e.g., “quando” e “qual” serviço deve ser despoletado - i.e., se deve ser contactado um AS, quer para serviços originados quer para serviços terminados).

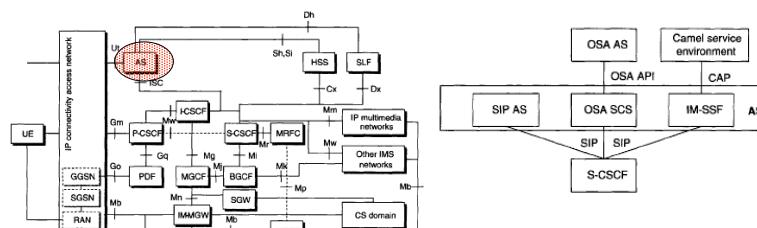


A arquitetura IMS: AS

Elementos da arquitectura:

• Funções de Serviço:

- Que disponibilizam serviços, possuem a lógica, dos serviços.
 - Residem na rede *home* do utilizador ou numa rede *3rd party*.
 - A interacção entre os AS e a rede IMS é feita através da interface ISC (protocolo SIP). Um AS possui capacidade para:
 - Processar (consumir e/ou alterar) mensagens SIP que lhe são enviadas.
 - Originar pedidos SIP.
 - Enviar informação de taxação.
 - A interacção entre ASs está fora do âmbito do IMS.



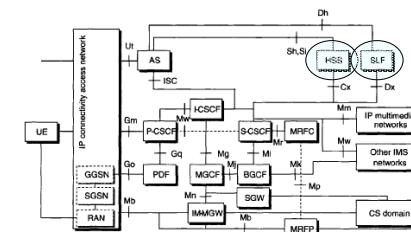
A arquitetura IMS: HSS

Elementos da arquitectura:

- Bases de dados

- *Home Subscriber Server (HSS)*

- Base de dados fundamental para toda a informação dos utilizadores (perfis): informação de registo, identidade(s):
 - Privadas (registo e autorização) e pública (através da qual se é contactado)
 - e serviços (informação para o disparo de serviços)
 - Funcionalidade de *Home Location Register (HLR)*

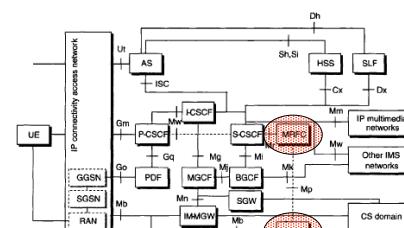


A arquitetura IMS: MRFC e MRFP

Elementos da arquitectura:

- **Funções de Serviço**

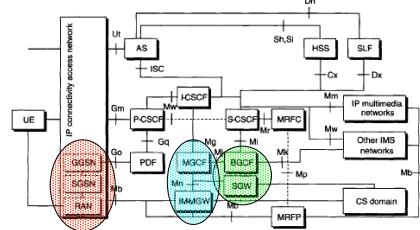
- *Media Resources Function Controller (MRFC)* e *Media Resources Function Processor (MRFP)*.
 - Conjuntamente oferecem serviços para controlar as connecções da media - e.g., conferências, anúncios, IVR.



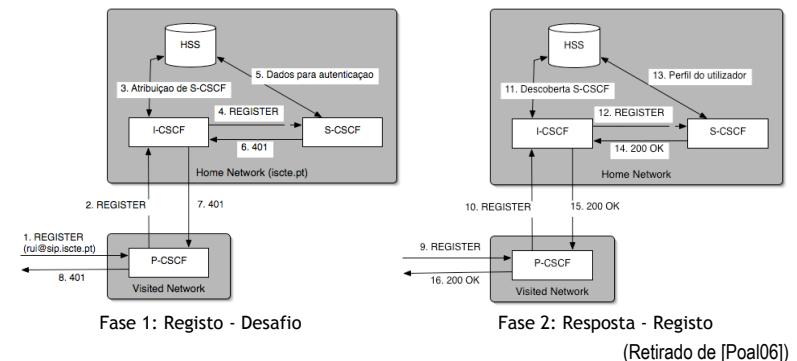
A arquitectura IMS: Gw

Elementos da arquitectura:

- Funções de Interligação:
 - Para a sinalização: *Breakout Gateway Control Function (BGCF)*
Signaling Gateway (SGW)
 - Para a media: *Media Gateway Control Function (MGCF)*
IM-Media Gateway (IM-MGW)
 - Para a rede de acesso: (e.g., *GGSN*, *SGSN*, *RAN*)



IMS: Registo

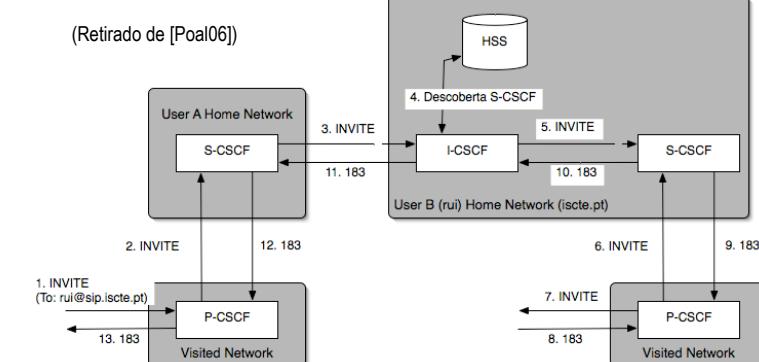


Depois de completo o registo:

- O UE e o I-CSCF sabem qual S-CSCF utilizar
- O S-CSCF tem o perfil do utilizador (e.g., critérios para disparar serviços)

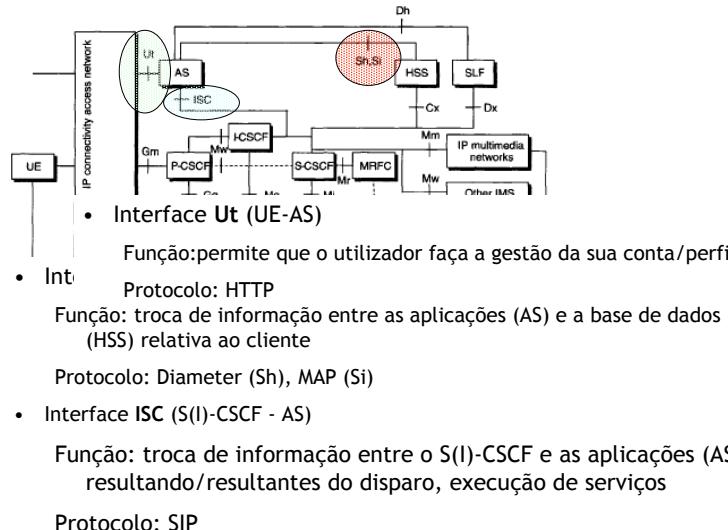
Questões: como se descobre o P-CSCF, como se descobre o I-CSCF ?

IMS: Inicio de Sessão

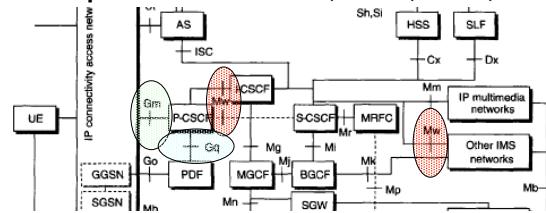


- Questões: como sabe o P-CSCF (de Visited A) onde se encontra o S-CSCF de A? como sabe o S-CSCF (de Home A) onde se encontra o I-CSCF de B?
 - Caso a mensagem INVITE (ou outra) corresponda aos critérios para o disparo de serviços os S-CSCF podem reencaminhar as mensagens SIP para ASs.
- Questão: como sabe o S-CSCF esses critérios?

IMS: Principais interfaces; Ut; Sh, Si; ISC



IMS: Principais interfaces; Gm; Mw; Gg



- Interface Gm, Mw (UE - P-CSCF, CSCF)

Função: troca de toda a informação de sinalização entre o terminal do utilizador (UE) e a P-CSCF, e entre os diferentes CSCFs na mesma rede ou redes diferentes

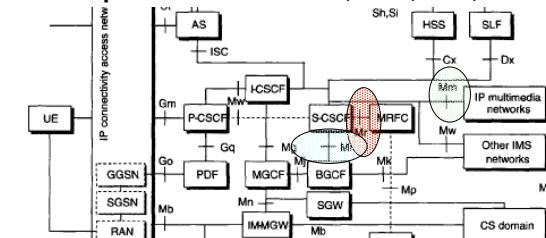
Protocolo: SIP

- Interface Gq (P-CSCF - PDF)

Função: troca de informação de sinalização relativa à política de acessos a recursos (e.g., largura de banda, atrasos, etc.) entre o P-CSCF e o Policy Decision Function (PDF)

Protocolo: Diameter

IMS: Principais interfaces; Mr; Mi; Mm



- Interface Mr (S-CSCF - MRFC)

Função: troca de toda a informação de sinalização entre o S-CSCF e o Media Resource Function Controller (e.g., utilizada para o controlo de servidores de media - caixas de voz, IVR)

Protocolo: SIR

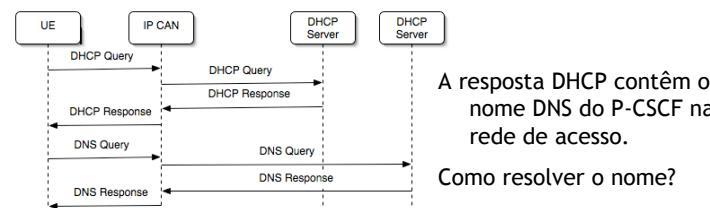
- Interface **Mi, Mm** (S-CSCF - BGCF, (I)S-CSCF - rede IP)

Função: troca de informação de sinalização quando à necessidade de utilizar uma outra rede externa não-IMS (IP ou CS)

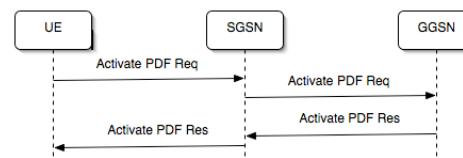
Protocolo: SIP (Mi), não especificado (Mm)

IMS: Descoberta do P-CSCF

- Configuração directa no UE (pouco recomendável)
 - Usando o DHCP (redes IP)



- Utilizando os protocolos SGCN, GGSN (redes GPRS)



IMS: Descoberta de nomes/domínios DNS

- **Questão:** como descobrir o I-CSCF numa determinada rede quando se pretende contactar um utilizador dessa rede ?

1. Utilizando um nome DNS exclusivo para SIP, e.g. `sip.iscte.pt` em `sip:ru@sip.iscte.pt`

- ## 2. Usando entradas (RR) de tipo NAPTR e SRV [RFC3263]:

- Cenário

- Existem duas máquinas na rede `iscte.pt` a funcionar como I-CSCF:
 - `sipseguro.iscte.pt` (SIPS sobre TCP, no porto 5060)
 - `sipseguro.iscte.pt` (SIPS sobre TCP, no porto 5060)

- A que correspondem as seguintes entradas no mater file DNS:

; nome class

iscte.pt IN NAPTR 50 "s" "SIPS+D2T" "" sips. tcp.iscte.pt

iscte.pt IN NAPTR 50 "s" "SIP+D2T" "" sip.tcp.iscte.pt

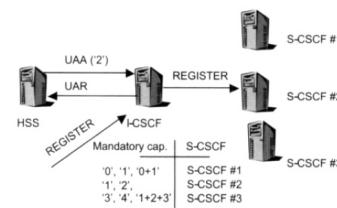
: nome class

sips tcp iscte pt IN SRV 0 1 5060 sinseguro iscte m

sips tcp:isctc.pt IN SRV 0 1 5060 sippnormal:isctc.pt

IMS: Selecção do S-CSCF

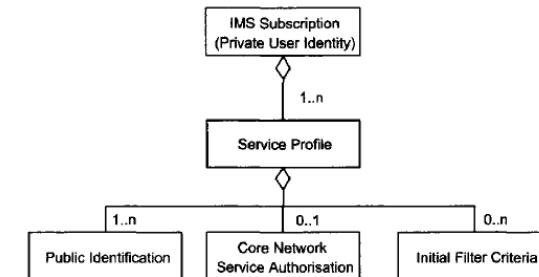
- Durante o registo
 - I-CSCF contacta o HSS indicando a identidade
 - Recebe uma lista de possíveis S-CSCFs e respectivas capacidades
 - Escolhe a mais adequada às características do utilizador. UE, etc.



- Quando um utilizador não registado recebe um pedido SIP: (ex. Serviço de tipo Terminating_unregistered).
 - O I-CSCF inicia uma troca de mensagens LIA/LIR (Location Information) em cuja resposta se encontra o S-CSCF que serve o utilizador.
 - Caso esta resposta não seja possível é devolvida uma lista de possíveis S-CSCFs utilizando o mesmo processo de escolha que no registo.

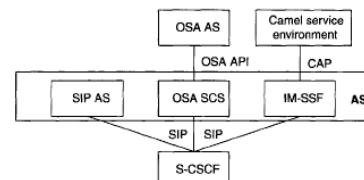
IMS: Perfil do utilizador

- Perfil do utilizador
 - Guardado permanentemente no HSS do seu operador
 - Transferido para um S-CSCF adequado quando necessário (registo, pedido para utilizador não registado).
- Conteúdo do perfil do utilizador:

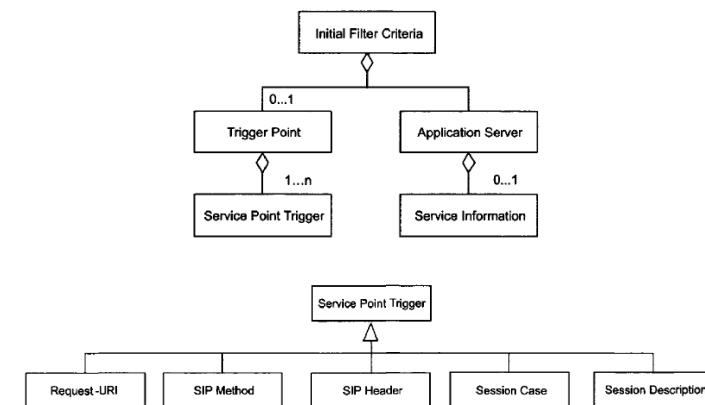


IMS: Provisão de serviços

- IMS não são serviços:
 - O IMS não é um serviço, é antes uma arquitectura (baseada em normas) para a provisão de serviços de telecomunicações sobre redes IP.
- Requisitos para a provisão de serviços por um operador:
 - Definir serviços ou conjuntos de serviços disponíveis.
 - Definição da informação associada a cada utilizador indicando que serviços usa, quais as regras/condições para a sua utilização e onde é prestado esse serviço (*initial filter criteria*).
 - "Disparar" os serviços, i.e., encaminhar as mensagens SIP para o servidor aplicacional (AS) adequado.



IMS: Initial Filter Criteria



IMS: Initial Filter Criteria (INVITE, Terminating_Unreg)

```

<IMSSubscription>
  <PrivateID> privatexyzjoe@ims.example.com </PrivateID>
  <ServiceProfile>
    <PublicIdentity>sip:joe.doe@ims.example.com</PublicIdentity>
    <PublicIdentity> tel:+358503334444 </PublicIdentity>

    <InitialFilterCriteria>
      <Priority>0</Priority>

      <TriggerPoint>
        <SPT><Method>INVITE</Method></SPT>
        <SPT><SessionCase> 2 </SessionCase></SPT>
      </TriggerPoint>

      <ApplicationServer>
        <ServerName>vmail@ims.example.com</ServerName>
        <DefaultHandling>l</DefaultHandling>
      </ApplicationServer>
    </InitialFilterCriteria>
  </ServiceProfile>
</IMSSubscription>

```

IMS: Initial Filter Criteria (INVITE, Terminating_Unreg)

```

<IMSSubscription>
  <PrivateID> privatexyzjoe@ims.example.com </PrivateID>
  <ServiceProfile>
    <PublicIdentity>sip:joe.doe@ims.example.com</PublicIdentity>
    <PublicIdentity> tel:+358503334444 </PublicIdentity>

    <InitialFilterCriteria>
      <Priority>0</Priority>

      <TriggerPoint>
        <SPT><Method>INVITE</Method></SPT>
        <SPT><SessionCase> 2 </SessionCase></SPT>
      </TriggerPoint>

      <ApplicationServer>
        <ServerName>vmail@ims.example.com</ServerName>
        <DefaultHandling>l</DefaultHandling>
      </ApplicationServer>
    </InitialFilterCriteria>
  </ServiceProfile>
</IMSSubscription>

```

IMS: Initial Filter Criteria (INVITE, Terminating_Unreg)

```

<IMSSubscription>
  <PrivateID> privatexyzjoe@ims.example.com </PrivateID>
  <ServiceProfile>
    <PublicIdentity>sip:joe.doe@ims.example.com</PublicIdentity>
    <PublicIdentity> tel:+358503334444 </PublicIdentity>

    <InitialFilterCriteria>
      <Priority>0</Priority>

      <TriggerPoint>
        <SPT><Method>INVITE</Method>, <SPT><SessionCase> 2 </SessionCase></SPT>
      </TriggerPoint>

      <ApplicationServer>
        <ServerName>vmail@ims.example.com</ServerName>
        <DefaultHandling>l</DefaultHandling>
      </ApplicationServer>
    </InitialFilterCriteria>
  </ServiceProfile>
</IMSSubscription>

```

IMS: Initial Filter Criteria (INVITE, Terminating_Unreg)

```

<IMSSubscription>
  <PrivateID> privatexyzjoe@ims.example.com </PrivateID>
  <ServiceProfile>
    <PublicIdentity>sip:joe.doe@ims.example.com</PublicIdentity>
    <PublicIdentity> tel:+358503334444 </PublicIdentity>

    <InitialFilterCriteria>
      <Priority>0</Priority>

      <TriggerPoint>
        <SPT><Method>INVITE</Method></SPT>
        <SPT><SessionCase> 2 </SessionCase></SPT>
      </TriggerPoint>

      <ApplicationServer>
        <ServerName>vmail@ims.example.com</ServerName>
        <DefaultHandling>l</DefaultHandling>
      </ApplicationServer>
    </InitialFilterCriteria>
  </ServiceProfile>
</IMSSubscription>

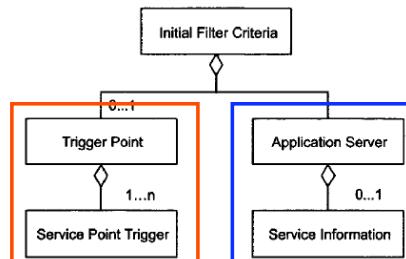
```

IMS: Initial Filter Criteria (INVITE, Terminating_Unreg)

```

<IMSSubscription>
  <PrivateID> privatexyzjoe@im
  <ServiceProfile>
    <PublicIdentity>sip:joe.do
    <PublicIdentity> tel:+3585
    <InitialFilterCriteria>
      <Priority>0</Priority>
      <TriggerPoint>
        <SPT><Method>INVITE</Method></SPT>
        <SPT><SessionCase>2</SessionCase></SPT>
      </TriggerPoint>
      <ApplicationServer>
        <ServerName>sip:vmail@ims.example.com</ServerName>
        <DefaultHandling>l</DefaultHandling>
      </ApplicationServer>
    </InitialFilterCriteria>
  </ServiceProfile>
</IMSSubscription>

```



`<ApplicationServer>`

`<ServerName>sip:vmail@ims.example.com</ServerName>`

`<DefaultHandling>l</DefaultHandling>`

`</ApplicationServer>`

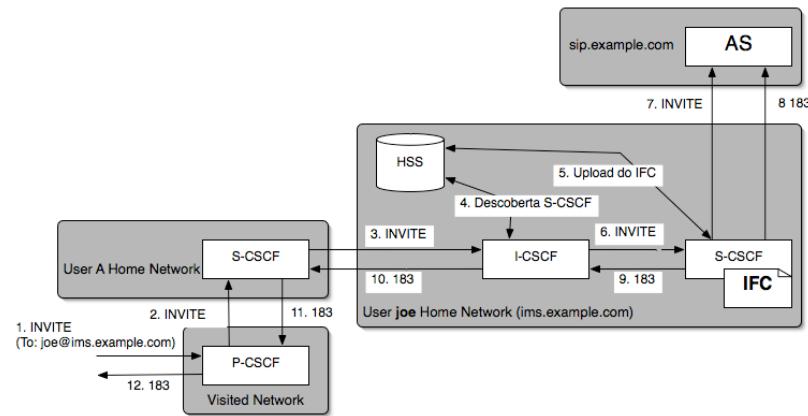
`</InitialFilterCriteria>`

`</ServiceProfile>`

`</IMSSubscription>`

IMS: Initial Filter Criteria (INVITE, Terminating_Unreg)

- O AS a funcionar como UE



IMS: Initial Filter Criteria (MESSAGE, Originating)

```

<IMSSubscription>
  <PrivateID> privatexyzjoe@ims.example.com </PrivateID>
  <ServiceProfile>
    <PublicIdentity> sms:+1555111333 </PublicIdentity>
    <InitialFilterCriteria>
      <Priority>0</Priority>
      <TriggerPoint>
        <SPT><Method>MESSAGE</Method></SPT>
        <SPT><SessionCase>0</SessionCase></SPT>
      </TriggerPoint>
      <ApplicationServer>
        <ServerName>sip:smss@ims.example.com</ServerName>
        <DefaultHandling>l</DefaultHandling>
      </ApplicationServer>
    </InitialFilterCriteria>
  </ServiceProfile>
</IMSSubscription>

```

`<ApplicationServer>`

`<ServerName>sip:smss@ims.example.com</ServerName>`

`<DefaultHandling>l</DefaultHandling>`

`</ApplicationServer>`

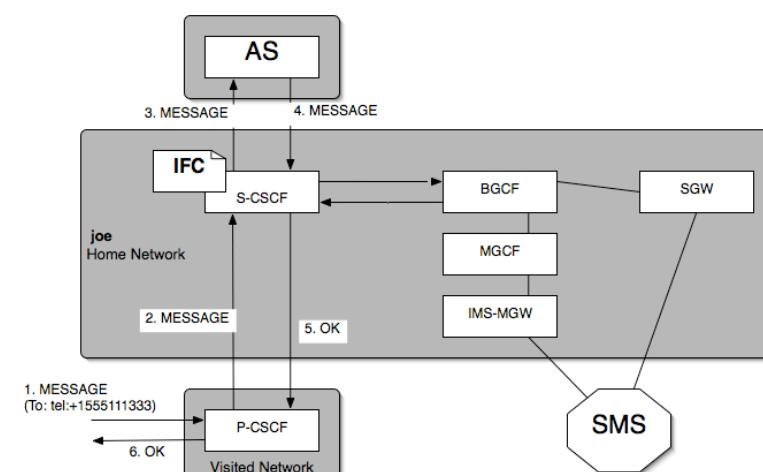
`</InitialFilterCriteria>`

`</ServiceProfile>`

`</IMSSubscription>`

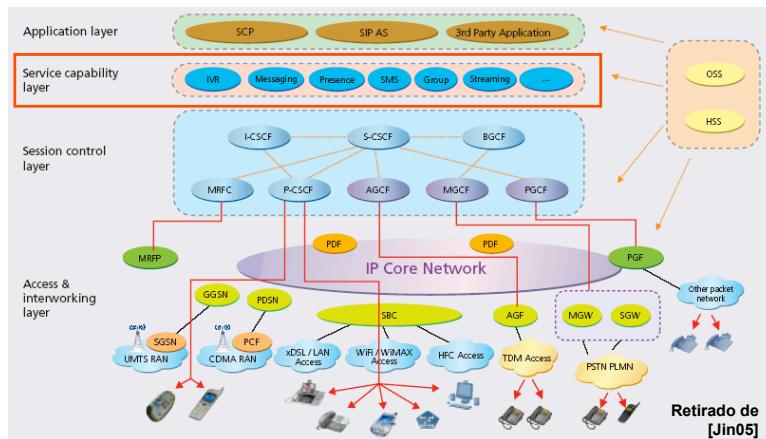
IMS: Initial Filter Criteria (MESSAGE, Originating)

- O AS a funcionar como SIP Proxy



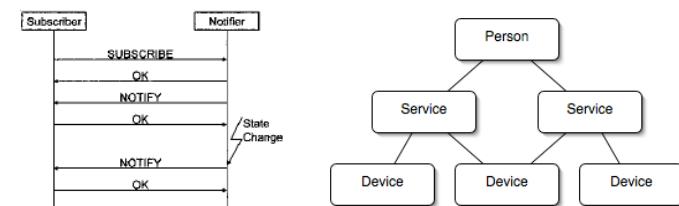
IMS: Serviços

- Recordar: “O IMS não é um serviço, é antes uma arquitectura (baseada em normas) para a provisão de serviços de telecomunicações sobre redes IP.”
 - No entanto ...



Serviço de Presença: SIP/SIMPLE, PDM

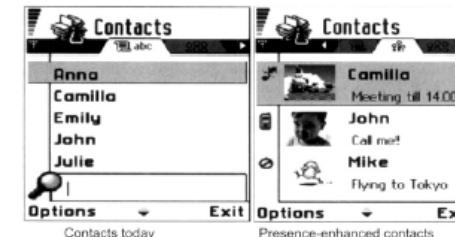
- A arquitetura para o serviço de presença no IMS é baseada na extensão *SIMPLE (Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions)* ao protocolo SIP no que se refere à presença: *A Presence Event Package for the Session Initiation Protocol (SIP)*, *RFC3856*.
 - A informação de presença é centrada no conceito de **presentity**: entidade (recurso) que associa informação de presença.
Existe um modelo de dados para descrever a presença:
A Data Model for Presence, *RFC4479*
 - Uma **presentity** é uma combinação de informação de presença de uma pessoa que tem associados um ou mais serviços, cada um destes serviços é prestado por um ou mais dispositivos.



Baseada no modelo geral do SIP para
subscrição/notificação de eventos.

Serviço de Presença

- Conhecer o estado de outros, dar a conhecer o meu estado.
"Serviço de presença": sistema que aceita, armazena e distribui informação de presença (RFC3856)"
 - Informação de presença:
 - Inicialmente bastante simples (online/offline),
 - evoluiu para informação mais rica (e.g., o que estou a ouvir, que UE estou a utilizar, até quando estou indisponível)
 - Informação de presença é apresentada e/ou utilizada por aplicações.



Retirado de [06]

Serviço de Presença: RPID

- O formato da informação de presença é o de um documento XML.

```
<presence entity="pres:someone@example.com">
<tuple id="p">
  <dm:person id="p1">
    <rpid:activities from="2005-05-30T12:00:00+05:00"
      until="2005-05-30T17:00:00+05:00">
      <rpid:note> Far away </rpid:note>
      <rpid:away/>
    </rpid:activities>

    <rpid:mood> <rpid:angry/> </rpid:mood>
    <rpid:place-is>
      <rpid:audio>
        <rpid:noisy/>
      </rpid:audio>
    </rpid:place-is>
    <rpid:place-type><lt:residence/></rpid:place-type>

    <rpid:sphere> bowling league </rpid:sphere>
    <rpid:status-icon>http://example.com/play.gif</rpid:status-icon>
    <rpid:time-offset>-240</rpid:time-offset>
    <dm:note>Scoring 120</dm:note>
    <dm:timestamp>2005-05-30T16:09:44+05:00</dm:timestamp>
  </dm:person>
</tuple>
```

Serviço de Presença: RPID

```

<tuple id="bs35r9">
  <status>
    <basic> open </basic>
  </status>
  <dm:deviceID> urn:device:0003ba4811e3</
  <rpid:service-class> <rpid:electronic/> </rpid:service-class>
  <contact priority="0.8"> im:someone@mobile.example.net </contact>
  <note xml:lang="en"> Don't Disturb Please!</note>
  <note xml:lang="fr"> Ne derangez pas, s'il vous plait</note>
  <timestamp>2005-10-27T16:49:29Z</timestamp>
</tuple>

<tuple id="ty4658">
  <status>
    <basic>open</basic>
  </status>
  <rpid:relationship> <rpid:assistant/> </rpid:relationship>
  <contact priority="1.0"> mailto:secretary@example.com </contact>
</tuple>

```

Serviço de Presença: RPID

```

<tuple id="eg92n8">
  <status>
    <basic>open</basic>
  </status>
  <dm:deviceID> urn:x-mac:0003ba4811e3 </dm:deviceID>
  <rpid:service-class> email</rpid:service-class>
  <rpid:status-icon>http://example.com/mail.png</rpid:status-icon>
  <contact priority="1.0">mailto:someone@example.com</contact>
</tuple>

<note>I'll be in Tokyo next week</note>

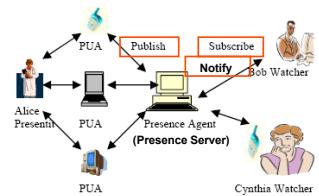
<dm:device id="pc147">
  <rpid:user-input idle-threshold="600"
  last-input="2004-10-21T13:20:00-05:00"> idle </rpid:user-input>
  <dm:deviceID> urn:device:0003ba4811e3 </dm:deviceID>
  <dm:note> PC </dm:note>
</dm:device>

</presence>

```

Serviço de Presença: Entidades (SIP/SIMPLE)

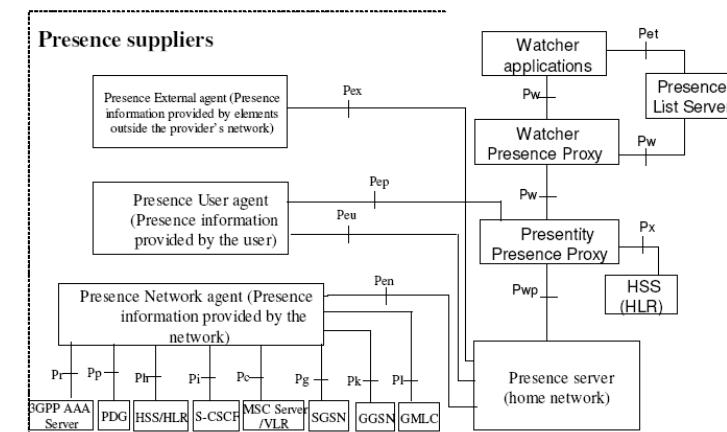
- **Presence User Agent (PUA):** gera informação de presença (PUBLISH) de um *presentity* (explicita/implicitamente). Um *presentity* pode ter vários PUA.
- **Presence Agent:** entidade lógica, pode estar colocalizada com outras entidades (PUA, proxy, registrar). Capaz de receber pedidos SUBSCRIBE, gerar mensagens NOTIFY indicando mudanças no estado de uma *presentity* (à qual tem acesso directa ou indirectamente).
- **Presence Server:** entidade física, pode funcionar como **Presence Agent** ou **Proxy** para pedidos SUBSCRIBE. Funcionando como PA têm de obter informação de presença da *presentity*.



- **Watcher:** entidade que pede (SUBSCRIBE) informação de presença de uma determinada *presentity* ao serviço de presença
- **Aplicações:** podem ser baseadas em presença ou ser aumentadas com informação de presença

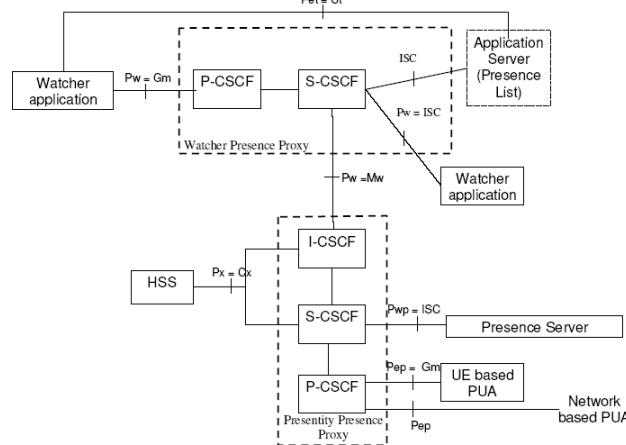
IMS Serviço de Presença: Arquitectura

- **Presence Suppliers:** diferentes entidades podem ser fontes de informação de presença.
- **Watchers:** diferentes entidades podem ser receptores de informação de presença.

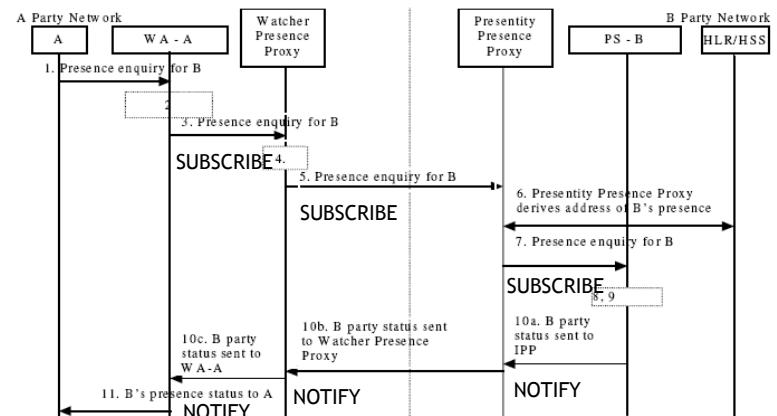


IMS Serviço de Presença: Arquitectura

- **Watcher e Presence Proxy:** O P-CSCF, I-SCSCF, S-CSCF podem ser usados como os pontos de contacto/entrada nas respectivas redes: do **watcher** e do **presence server**

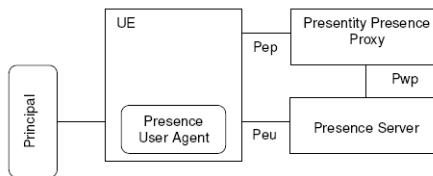


Presença IMS: Recipientes de informação Subscrição

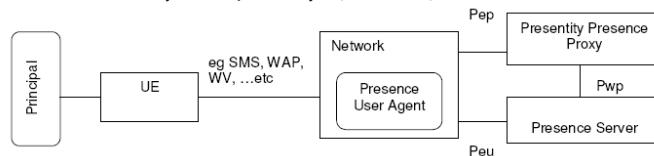


Presença IMS: Fontes de informação

- **Presence User Agent (PUA) no terminal:** O UE está directamente ligado à rede IMS, contém o PUA e fornece informação de presença (PUBLISH)

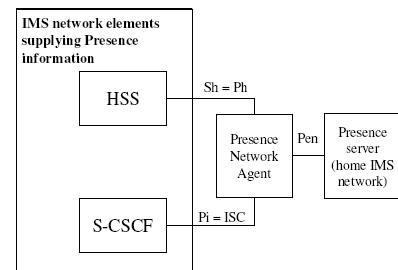


- **Presence User Agent (PUA) na rede:** O UE não contém o PUA, este encontra-se numa entidade da rede que recebe informação do UE e gera/fornecer informação de presença (PUBLISH)



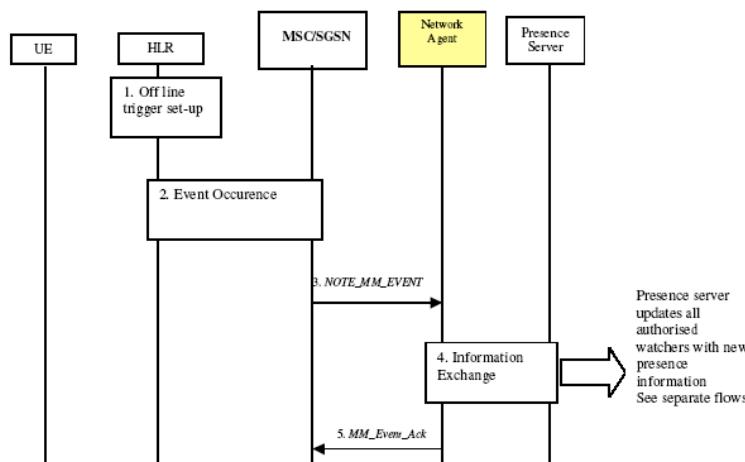
Presença IMS: Fontes de informação

- **Presence Network Agent (PNA):** um PA que se encontra na rede e que de acordo com outro tipo de informação gera/fornecer informação de presença (PUBLISH)

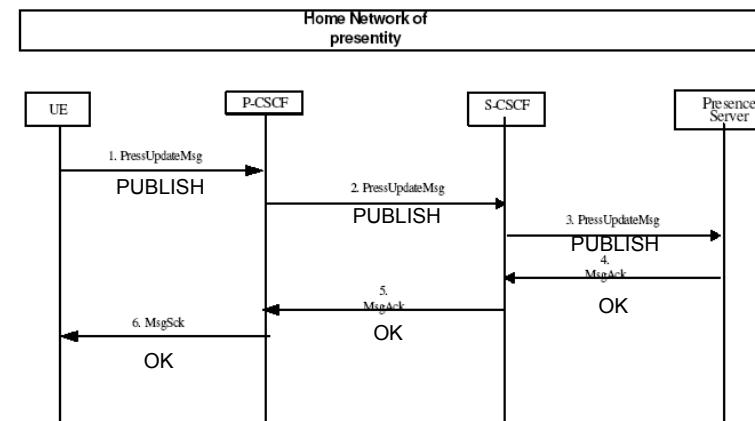


- **Exemplo 1 (fonte HSS):** Agenda pessoal permite indicar o estado de uma pessoa (ex. em reunião)
- **Exemplo 2 (fonte S-CSCF):** um terminal desliga-se da rede

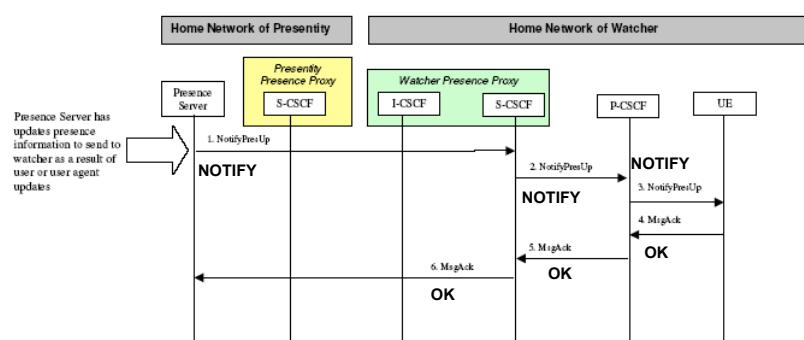
Presença IMS: Fontes de informação



Presença IMS: Publicação de presença



Presença IMS: Notificação de presença



Presença IMS: Subscrição/Notificação

