Lappeenranta University of Technology
Department of Information Technology

Service Architecture in Mobile IP Telephony Network

The topic of the master's thesis has been confirmed by the Department Council of the Department of Information Technology on 14 June 2000

Examiner: Professor Valery Naumov

Supervisors: Teemu T. Hänninen, Nokia Networks Oy
Minja Kolu, Nokia Networks Oy

Author: Evgeny Sobenin _____
Helsinki 31 October 2000

Author's address: Mannerheimintie 134 A 10
00270
Helsinki
Phone: 040-7008142

Abstract

Lappeenranta University of Technology

Department of Information Technology

Evgeny Sobenin

Service Architecture in Mobile IP Telephony Network

Master's thesis
Year of completion: 2000

61 pages, 18 figures, 1 table

Examiner: Professor Valery Naumov
Keywords: Service architecture, WIN, 3G, IP Telephony.

The most important thing that customers are expecting from new technology are new services. That is the main reason which makes them pay their money and start to use the technology. Thus service architecture of new network is the very important for the success of the whole project.

This document concentrates on service architecture for 3G Mobile IP Telephony Network. The description of the network reference model is given. The network services are shown and described.The implementation issues are presented and discussed. The WIN concept, which is required for US market, is described and the implementation issues are discussed as well. Finally, the problem of the pre-paid callers accounts recovery is considered and WIN solution is presented.

Tiivistelmä

Lappeenrannan Teknillinen Korkeakoulu
Tietotekniikan osasto

Evgeny Sobenin

Matkapuhelinjärjestelmien IP-verkkojen palveluarkkitehtuuri

Diplomityö
Työn valmistumisvuosi: 2000

61 sivua, 18 kuvaa, 1 taulukkoa

Tarkastaja: Professori Valery Naumov

Hakusanat: palveluarkkitehtuuri, WIN, 3G, matkapuhelinverkko

Uudet palvelut ovat tarkeinta, mita asiakkaat odottavat uudelta teknologialta.Se on paaasiallinen syy siihen, etta asiakkaat ovat valmiita maksamaan uudesta teknologiasta ja kayttamaan sita. Sen vuoksi uuden verkon tuoma uusi palveluarkkitehtuuri on hyvin tarkea koko projektin onnistumiselle.

Tama dokumentti keskittyy kolmannen sukupolven matkapuhelinverkkojen palveluarkkitehtuuriin, jonka viitemallista annetaan kuvaus. Verkon palvelut esitellaan ja kuvaillaan. Toteutukseen liittyvia asioita selostetaan. USA:n markkinoilla tarvittava WIN konsepti kuvataan ja sen toteutuksesta annetaan myos kuvaus. Lopussa kuvataan Pre-Paid tilaajien laskutustietojen kasittelya WIN konseptissa elvytystilanteessa.

Acknowledgements

This Master's thesis has been made in Nokia Networks Mobile Switching business unit in Helsinki. I wold like to thank all people who have helped me to accomplish this work. The thesis has been guided by Minja Kolu and Teemu T. Hänninen. I would like to thank them for the comments and support during my work. Especially I would like to thank Minja for the comments and advices that really helped me in my work. Your comments became a valuable input for my thesis.

Professor Valery Naumov from Lappeenranta University of Technology has been my examiner and supervisor. I would like to thank him for it.

I would like to dedicate this master's thesis to my wife, Natasha. You are the main reason that makes me improve myself.

Helsinki, Finland, 31 October 2000 _____

Evgeny Sobenin

Table of contents

Abbreviations

3G	Third Generation
3GPP	3G Partnership Project
AC	Authentication Center
ACF	Authentication Control Function
APPSE	Application Server
ATSI	Any Time Subscription Information
ATM	Any Time Modification
BCSM	Basic Call State Model
BS	Base Station
CAMEL	Customised Applications for Mobile network Enhanced Logic
CCDIR	Call Control Directive
CCF	Call Control Function
CPS	Call Processing Server
CPL	Call Processing Language
CS	Circuit Switched
CSCF	Call State Control Function
CSI	CAMEL Subscriber Information
GPRS	General Packet Radio Service
DFP	Distributed Functional Plane
DNS	Domain Name Server
DP	Detection Point
EDP	Event Detection Point
EDP-N	Event Detection Point – Notification
EDP-R	Event Detection Point – Request
EIR	Equipment Identity Register
HLR	Home Location Register
HSS	Home Subscriber Server
IN	Intelligent Network
INAP	Intelligent Network Application Part
IM	IP Multimedia
IP	Internet Protocol/Intelligent Peripheral
IPT	IP Telephony
FE	Functional Entity
LRF	Location Registration Function
MACF	Mobile Station Access Control Function
MC	Message Center
MGCF	Media Gateway Control Function
MGW	Media Gateway
MS	Mobile Station
MSC	Mobile Switching Center
MSRN	Mobile Station Roaming Number
MT	Mobile Terminal
NCSD	Notify Change of Subscriber Data
NE	Network Entity
NRM	Network Reference Model
OSA	Open Service Architecture
PIC	Point In Call

PPC	Pre-paid Charging
PS	Packet Switched
R-SGW	Roaming-Signalling Gateway
RACF	RadioAccess Control Function
RCF	Radio Control Function
RTF	Radio Terminal Function
SCP	Service Control Point
SCF	Service Control Function
SCEF	Service Creation Entity Function
S-CSCF	Serving CSCF
SDF	Service Data Function
SGW	Signaling Gateway
SIP	Session Initiation Protocol
SLP	Service Logic Program
SLPI	Service Logic Program Instance
SMAF	Service Management Access Function
SME	Short Message Entity
SMF	Service Management Function
SN	Service Node
SPD	Subscriber Profile Database
SRF	Special Resource Function
SS7	Signalling System number 7
SSF	Service Switching Function
TAL	Trigger Address List
TDP	Trigger Detection Point
TDP-N	Trigger Detection Point – Notification
TDP-R	Trigger Detection Point – Request
TE	Terminal Equipment
TLDN	Temporary Locator Directory Number
UDP	User Datagram Protocol
UMS	User Mobility Server
UMTS	Universal Mobile Telecommunications System
UNI	User-Network Interface
VLR	Visitor Location Register
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WIN	Wireless Intelligent Network

1. Introduction

Nowadays the 3G mobile IP telephony network concept is rapidly growing and the working 3G networks are about to became reality in nearest future. Of course, when new concept is introduced, the main question for the customers is: "What are the benefits ?" It's clear that new technology should offer new possibilities for the subscribers, and if those possibilities will satisfy the needs, the customers would pay for that. From that point of view, the services offered by new technology are the main result of implementing this technology, the "tool" for getting money from customer.

But the things are such that when the new technology is under development, the implementation starts from the very "core" elements, and services are the last element to be added to the system. And of course it's not easy to predict which services would be interesting for the customer, what are the needs. The network should include efficient mechanisms for service operations,in other words, network should have efficient service architecture.

The subject of this thesis is service architecture for 3G mobile IP telephony network. The structure is as follows:

Chapter 2 contains the description of the network which is the basement of the services. In chapter 3 the services for 3G network are introduced. Chapter 4 contains the description of the Wireless Intelligent Network concept. WIN support is required for US market. Chapter 5 describes the WIN technology mapping to 3G and discusses the issues of pre-paid callers recovery, which is very important service for the future networks, and WIN capabilities to solve that recovery problem. Finally, chapter 6 concludes the thesis and suggest some ideas for future work.

2. Third generation Mobile IP Telephony Network

2.1 Network Reference Model

The following picture describes the network reference architecture:

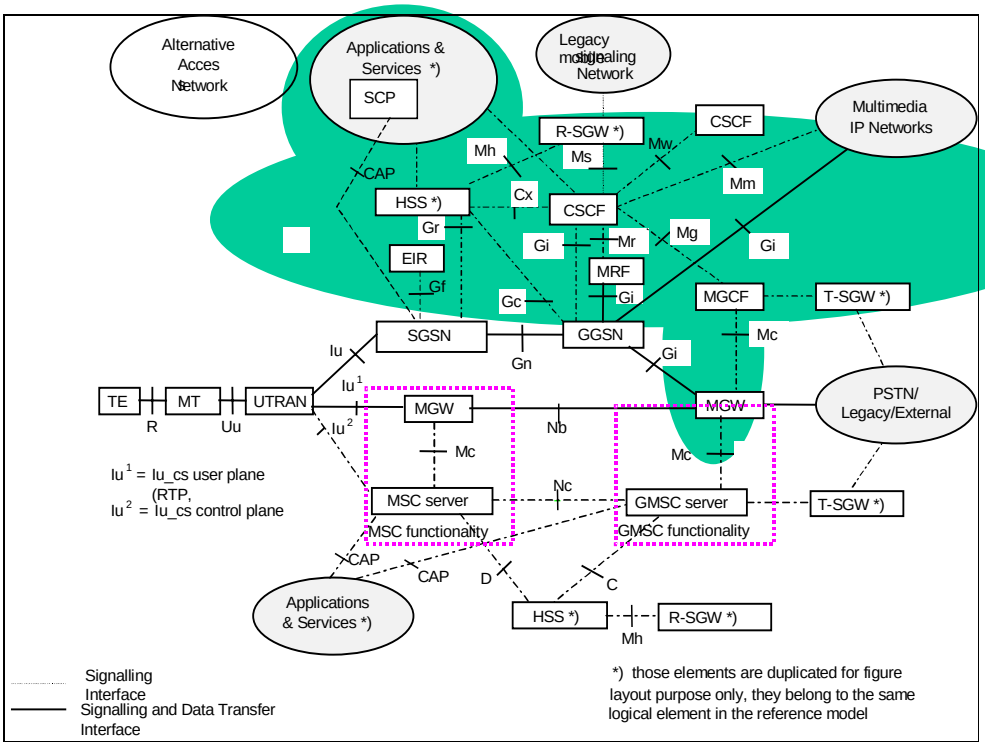

Figure 1: Network reference architecture

First phase of the implementation consists of the following network elements: CPS, HSS/HLR, MGCF/MGW and APPSE

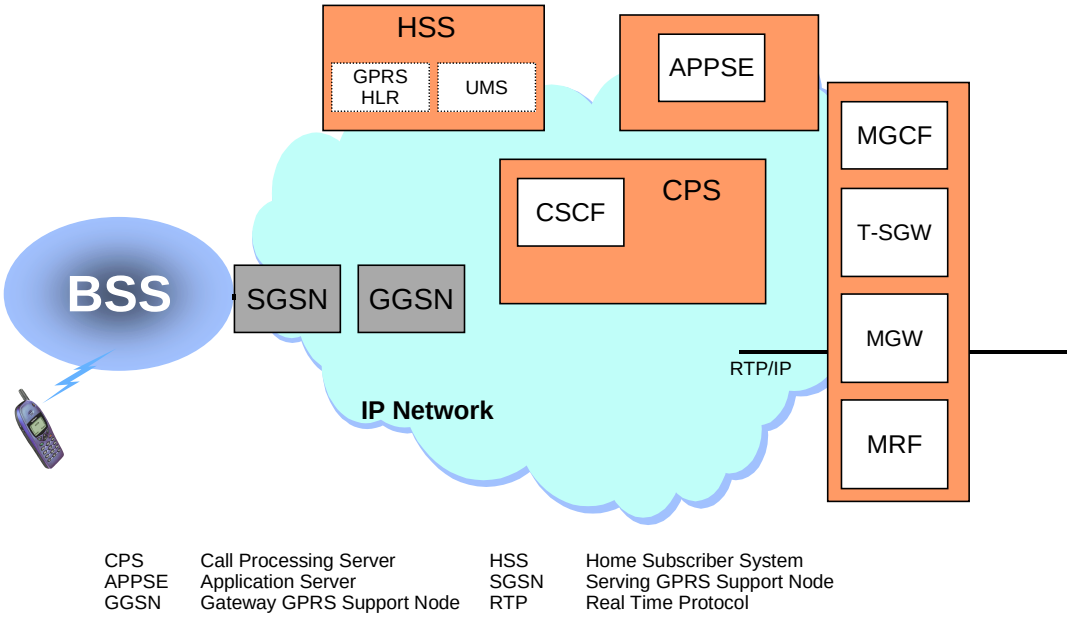

Figure 2: All-IP functionality mapping to products in first release

2.2 HSS

The Home Subscriber Server (HSS) is the master database for a given subscriber and the main subscriber database in the network. It contains all necessary subscriber information. It is responsible for keeping a master list of features and services (either directly or via servers) associated with a subscriber, and for tracking of location and means of access for its subscribers. It provides subscriber profile information, either directly or via servers. It is analogous to the Home Location Register (HLR), as defined in GSM, but differs in the fact that it needs to also communicate via new IP based interfaces. Like the HLR, the HSS contains or has access to the authentication centers / servers.

HSS consists of 3G HLR and User Mobility Server UMS. 3G HLR stores PS and CS related subscriber data. UMS stores IM subscriber profile and location information.

2.2.1 UMS

The overall responsibility of the UMS part of the HSS is to take care of the application level mobility management (i.e. keep the track of the serving CSCF). It also behaves as a primary store of application level service profile. The UMS has an essential role in the MT transactions and registration procedure. UMS also updates changes in subscriber profile to S-CSCF when needed.

The UMS functions are:

- mobility management
- subscriber data storing
- location query management
- security

2.2.2 3G HLR

Basically the 3G HLR manages the functions of CS HLR and GPRS HLR.
The functions are:

a) CS functions:

- mobility management
- subscriber data storing
- routing information providing
- security

b). PS functions:

- GPRS mobility management
- subscriber data storing
- routing information providing
- security

2.3 CPS

The Call Processing Server provides control of IP Telephony services. The CPS contains IP Telephony call-state models that co-ordinate the call set-up with the help of other network elements such as the APPSE. The CPS is the element to which IP Telephony terminals register and through which call control signaling (SIP) is conveyed. The CPS has interfaces towards the IP Telephony application servers (APPSE) (CAPv3)..
CPS covers CSCF function.

2.3.1 CSCF

CSCF is the main call control element of IP-telephony network. CSCF provides call control service to IP-telephony subscriber. CSCF also provides service capabilities which are used by application logic to provide value added services to IPT subscribers. CSCF holds information of registered IPT subscribers at SPD.

The CSCF:

- accepts and process registration request of IP-telephony subscriber
- provides function capabilities to application services
- provides service control signalling
- provides mechanisms to trigger to application services
- querying the subscriber's location
- provides address handling
- reports call events for billing, auditing, intercepting or other purpose
- invokes location based services relevant to the serving network
- provides call set-up/termination and state/event management

2.3.2 SPD

Subscriber Profile Database is IP-Telephony level temporary register holding subscriber's profile information and (temporary) transport address. Since subscriber registers to CSCF some subscriber related information must be stored in CSCF. SPD is this storage. SPD also participates in the authentication of IPT subscription.

The functions of SPD are:

- handling of registration, unregistration and location cancellation
- providing the Call Control with service and location data
- storing the subscriber's data and service profile which is downloaded from the UMS in serving-CSCF (S-CSCF)

3. Services in 3G

3.1 Application server

The Application Server (APPSE) is the core network element responsible for producing the IP Telephony services. It provides an environment for IP Telephony service creation, management and execution. APPSE also contains a database storing the full service information for each IPT subscriber. It provides user interface for IPT subscribers to value added service activation and management.

The following fogure shows how the APPSE is positioned in the network:

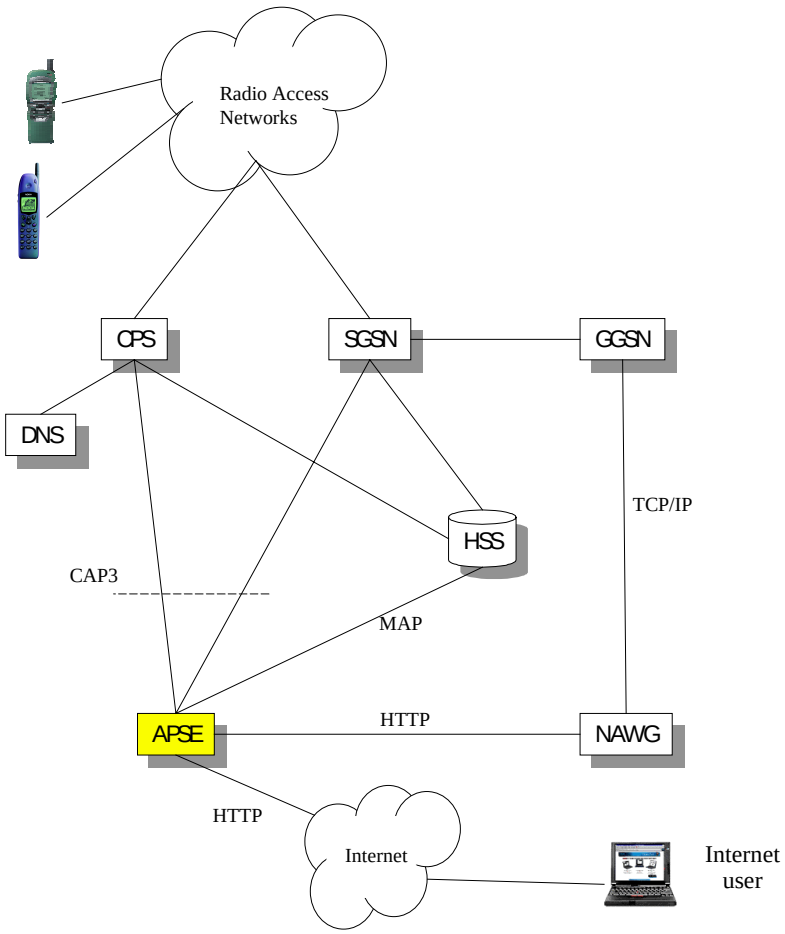

Figure 3: The position of the application server (APPSE) in the network

3.1.1 APPSE functions

Service execution.

CPS may request for IPT services during call setup using mechanims provided by CAMEL phase 3. CPS sends service requests to APPSE in case subscriber profile in HSS contains a suitable CAMEL trigger. APPSE receives the service requests, initiates the correct IPT services according to its subscriber database and returns instructions to CPS using service capabilities available in CAMEL phase 3.

Service creation.

Services are created only by the operator using internal service creation machinery provided by APPSE.

Service provisioning

Subscriber's services are provisioned to the database of the APPSE using the normal operator's service management tools.

Service activation and management

Service activation here refers to the event after which calls to a specific IPT subscriber need an execution of a service in the APPSE. Service activation may be done by the operator using internal service management tools (e.g. Prepaid service) or by IPT subscriber himself when taking the service into use (e.g. Call Forwarding) via a user interface. In both cases APPSE marks the service to be active in its subscriber database and sends an update request to HSS to set a suitable CAMEL trigger to be active for that specific user.

In case service information (e.g. Call Forwading Number) is changed, APPSE updates the data in its database. Service information may be changed by operator or the user (via user interface). If services of a subscriber is removed or changed so that its starting point in call setup should be changed, APPSE sends an update request to HSS to update CAMEL trigger information.

User interface

APPSE provides the IPT user a user interface via which he may activate/deactivate services or modify the operation of the services. The default user interface offered by

APPSE is an internet interface allowing an IPT user to modify services with a Web browser (i.e. using html). APPSE also interfaces WAP gateway and via this WAP gateway services may also be managed using WAP applications.

3.2 Services and service capabilities

The core network elements CPS & HSS offer a set of service capabilities for IPT applications which are built in the Application Server (APPSE). IPT value added services in APPSE may use these service capabilities (e.g. call control, subscriber location information, user interaction) to control the functions performed by the core network elements CPS & HSS during registration and call processing.

3.2.1 Service capabilities

Service capabilities offer access to network resources for for services and applications built in APPSE. They hide the implementation of the basic core network functionality and offer a unified control interface for APPSE.

The service capabilities may be grouped as follows:

- Call control
- Network user location
- User interaction
- Charging

3.2.1.1 Call control

Service capabilities of call control may be separated to non-call-related and call-related capabilities. Non-call-related capabilities are mainly offered by the HSS functionality of the core network; however, some CSCF functionality may also be needed. The call-related capabilities are offered by the CSCF functionality.

Non-call-related capabilities include the following:

- Management of service / application triggers arming / provisioning. Static and dynamic arming / provisioning of services is required already now. Static arming / provisioning means creating trigger data and attaching it to user profiles or other relevant data ,i.e. configuration of HSS and CSCF. Dynamic arming means that HSS offers a possibility for applications to activate / passivate trigger data directly via e.g. CAP interface (this can be done with CAMEL AnyTimeModification operation).
- CSCF registration. Reporting of the user's registration / deregistration to a S-CSCF should be supported in future. At the moment registration is not supported.
- Screening of service initiation towards Application Servers. Call gapping functionality is not supported at the moment. In future support is needed.
- Management of user data in HSS. An application may request the HSS to notify itself, if user's data in HSS is changed (e.g. CAMEL NCSD, Notify Change of Subscriber Data, operation). An application may also request the HSS to return user profile information (e.g. CAMEL ATSI, Any Time Subscription Information, operation). Additionally, an application may request the HSS to change some data in user profile (e.g. CAMEL ATM, Any Time Modification).

Call-related capabilities include the following:

- Establishing a control relationship. The core network initiates control connection towards a service (inside a SCP or AppSE) when the conditions specified by the trigger (e.g. detection point of a Basic Call State Model, called party number, etc.) related to the service are met. This is a basic functionality which must be supported from the beginning. However, the set of detection points supported may vary due to time. At the moment the call related detection points specified in CAMEL phase 3 specification are supported. Also the data conveyed to the service may vary.

- Event monitoring. If an active service (control relationship has been initiated and it is active) requests dynamically an event report for itself, when given detection points are met in the same call, encountering of these detection point must be reported to this service by the core network. This is a basic functionality which must be supported from the beginning. However, the set of detection points supported may vary due to time. At the moment the call related detection points specified in CAMEL phase 3 specification are supported. Also the data conveyed to the service may vary.
- Routing control. A service may give an instruction to redirect the call to another called party number (e.g. CAMEL Connect operation). A service may also change the data in CSCF without redirecting the call (e.g. CAMEL ContinueWithArgument operation). This is a basic functionality which must be supported from the beginning.
- Collection of additional address information. A service may request the core network to collect additional address information (e.g. CollectInfo CoreINAP operation). This basic functionality is not supported (not supported in CAMEL).
- Release. A service may instruct the core network to release the call and resources associated with it. This is a basic functionality which must be supported from the beginning.
- Release connection to a service. A service may ask the core network to close the connection to a service without disconnecting the call (e.g. CAMEL Cancel operation). This is basic functionality which must be supported from the beginning.
- Supervising the connection between a service and core network. The service may check the existence of a connection between the service and the controlled Basic Call State Model in CSCF (e.g. ActivityTest CAMEL operation). This is a basic functionality which must be supported from the beginning.
- Reporting call specific information to a service. A service may ask the core network to return call specific data (e.g. CAMEL CallInformationRequest). This is a basic functionality which must be supported from the beginning.
- Time supervision of a call. A service may instruct core network to either release the call resources or send a report to the service, when a time limit specified by the service has been reached. This is a basic functionality which must be supported from the beginning.

- Reporting of call failures. The CSCF is able to notify the services of a failure / abort of a call. However, the services (e.g. CAMEL) may not always get this notification due to protocol specific limitations. This is a basic functionality which must be supported from the beginning.
- Call Party Handling. A service may request the CSCF to add new call parties, disconnect call parties, change connection of existing call parties in a stable call.
- Initiate Call Attempt. A service may request the CSCF to initiate a new call to a given destination.

3.2.1.2 Network user location

A service may ask the location of a user from the core network. The location may be e.g. a SPD/CSCF address, geographical location parameters or some other means of identifying the user location. Since user information is located in the HSS, this capability is offered by HSS functionality if offered by core network. CAMEL has Any Time Interrogation operation for requesting the user location.

At the moment core network does not support requests for user location. The core network (HSS) should be able to report the location of the user in some form (e.g. the address of the S-CSCF the user is registered to). Furthermore, a service should be able to notify a service of a change in the location of the user, i.e. report the new location, if requested. These requirements are set by OSA.

3.2.1.3 User interaction

User interaction capabilities of core network are offered by the CSCF functionalities of the core network.

User interaction capabilities include the following:

- Connection to user interaction resources. A service may request the core network to connect a user to an external network element capable of user interaction (e.g. CAMEL Establish Temporary Connection), or to connect the user to the user interaction resources of the core network itself (e.g. CAMEL Connect To Resource operation).

- End user initiated user interaction. User interaction initiated by an end user towards a service is not supported now in core network (capabilities of the terminal and its service execution environment are an outside scope of this document).
- Sending info to user. At the moment info sent to end user is according to CAMEL phase 3 implementation, i.e. voice announcements from external Service Resource Point. In future also text strings should be supported.
- Collecting information from user. At the moment info collection is according to CAMEL phase 3 implementation (PromptAndCollect). In future collection of text strings may be required.
- Release of user interaction resources. The service may request the core network to release the resources reserved for user interaction. This is already supported.

3.2.1.4 Charging

Charging capabilities are offered by the CSCF functionalty.

Charging capabilities include the following:

- Setting Advice Of Charge parameters. A service may request the setting of the parameters used for AdviceOfCharge (e.g. CAMEL SendChargingInformation). This is not supported now. Support may be needed in future.
- Setting Call Detail Records data. A service may put data to the off-line charging records made for the call (e.g. CAMEL Furnish Charging Information). This functionality is already supported.
- Changing the network specific charging. The service may request the changing of the charging parameters of the network element (either replace the charging parameters or decrease/increase charging). This INAP-like charging is not supported at the moment (not supported by CAMEL at all).
- Setting limits for the call based on network specific charging. A service may request an event from the core network when the charging made locally in the CSCF reaches some limit, e.g. amount of money. This is not supported yet.

3.2.1.5 Service capabilities required by OSA

Open Service Architecture promoted by 3GPP consists of three parts:

- Applications (e.g. VPN) which are run in Application Servers.

- Framework providing applications with basic mechanisms that enable the application to make use of service capabilities in the network.
- Service Capability Servers**,** providing the applications the service capability features which are abstractions from underlying network functionality.

At the moment, the core network does not fully implement any of those parts; it is assumed that a CAMEL CSE is the Service Capability Server offering the service capability features to the applications via OSA interface. The core network mainly offers network service capabilities for CSE.

In case the core network offers the OSA interface towards applications in future, that is, core network implements the Service Capability Server functionality, the core network must be able to registrate and maintain its supported network service interfaces to the framework. Framework needs this in order to support service capability feature discovery made by applications. In addition, the core network must be able to provision and activate triggers set by applications through OSA interface, e.g. dynamically accept provisioning of a new service to HSS.

Depending on how OSA is implemented, it is possible that the core network should also support framework services in future. The framework service capabilities offered to applications include e.g. the following:

- Authentication. The application must authenticate framework and vice versa. Authentication is needed before any other usage of OSA interface.
- Authorisation. After authentication, application needs to find out what it is allowed to do.
- Discovery of framework and service interfaces. After authentication the applications need access to framework services.
- Establishment of a service agreement. Before interacting with a network service capability feature, a service agreement must be established.
- Access to network service capability features. The framework must provide the access control functions to authorise the access to service capability features or service data for any API operation.

3.2.2 Services

Services use service capabilities located in HSS and CSCF in order to control the functionality of the core network according to service logic run in the Application (APPSE).

The core network stores information of the provisioned active IPT services in the database of the APPSE. The HSS database (in subscriber's profile) and the CSCF data (e.g. in analyses) contain information which identifies whether or not a service inquiry should be sent to APPSE. The HSS/CSCF service capabilities ensure that when an event (e.g. a detection point is met during call setup, a user registrates to CSCF, etc.) specified by the provisioned active service occurs, the service will receive a report from the core network.

The CSCF locate in the visited network when user is roaming. This means that subscriber specific network service capabilities locate in the visited network CSCF when the user is roaming. Since the SCP giving instruction is in the home network, architecture is similar as in CAMEL.

3.2.2.1 Control Interface Protocols

CAMEL

CAMEL will be the main external control interface supported towards core network. Restricted CAMEL phase 3 support will be built already in near future.

OSA, Parlay

Open Service Architecture (OSA) promoted by 3GPP and Parlay promoted by Parlay Group present the (near) future candidates for a control interface towards CPS. The concept given by these mechanisms allows easy outsourcing of service implementation to network elements connected to a Corba based network.

OSA and Parlay will be the protocols giving the proprietary enhancements for service implementation in the home network.

INAP

INAP will not be supported in the CPS, mainly because it was made for controlling **fixed** switches.

SIP

SIP, Session Initiation Protocol, is a basic protocol used in IP world. It may also be used as a control protocol (e.g. between CSCF and SCP) for certain applications.

CPL

CPL, Call Processing Language, offers a script based mechanism to control the core network. The support of CPL is under discussions.

WIN

WIN protocol is a requirement from the American market. It won't be supported in near future. The following parts of this document are dedicated to WIN decsription and analysis, which might be useful for WIN support in later releases.

4. WIN in general

The Wireless Intelligent Network (WIN) is a network which supports the use of intelligent network capabilities to provide seamless terminal services, personal mobility services and advanced network services in the mobile environment.

Intelligent network capabilities are all those functional capabilities which support creation and execution of service logic programs which reside outside of switching equipment, but work in collaboration with the switching equipment based upon a common definition of call models and protocols. These service logic programs may utilize data resources and physical resources which also reside outside of the switching equipment.

Terminal mobility services are services created using intelligent network capabilities to serve customers with mobile terminals. A set of these services will be associated with each mobile terminal based on the capabilities of the terminal and subscription selections. Some prerequisites of providing these services are the abilities to identify and authenticate the terminal and to provide seamless operations capabilities between wireless and wireline networks.

Personal mobility services are services created using intelligent network capabilities to serve customers who are mobile. A set of these services will be associated with each customer based on personal subscription selections. The customer may utilize a variety of mobile and fixed terminals at different locations. Some prerequisites of providing these services are the abilities to:

- identify and authenticate the person (subscriber) who has been provisioned for the service
- provide seamless operations capabilities among the wireless, fixed and other networks (e.g., broadband, internet, data networks)
- provide a unique set of services to the subscriber based on the subscriber's access point to the WIN service

Advanced network service has the functionality to identify the capability of the serving network, to provide service based on the network and terminal capability, and to provide seamless service mobility between wireless and wireline networks.

The basic difference between terminal mobility service, personal mobility service and advanced network service is as follows:

Terminal mobility services: services based on the terminal capability irrespective of the terminal user.

Personal mobility services: services based on personal needs or business entity needs irrespective of terminals or networks.

Advanced network services: customized services which can be provided ubiquitously in home or roaming networks (wireless or wireline).

Service management functionality is used to provision and manage the service control functionality, the service data functionality, and the specialized resource functionality in the network. Service creation functionality is used to create services. Service management and service creation functionality may use standardized interfaces. However, the ability of a service subscriber to interact directly with subscriber-specific service management information will not be excluded or constrained for WIN.

4.1 Distributed Functional Plane

The ditrubuted functional plane (DFP) defines the WIN architecture in terms of functional entities (FEs), each of which performs distinct actions in the network. A grouping of actions across one or more FEs, when coordinated by communication flows, provides the required WIN service execution.

The WIN DFP provides a different view of the network than is provided by the wireless network reference model (NRM). The NRM defines network entities and the associated interface reference points that may logically comprise a wireless network. The WIN DFP identifies FEs that perform distinct actions in the network. Multiple FEs can be included in a single network entity.

The scope of the DFP architecture for WIN is driven by the requirements of desired wireless services and is constrained by the capabilities of the embedded base of evolvable network technology.

The functions required to support the desired wireless services include:

- end user access to call and service processing
- service invocation and control
- end user interaction with service control
- service management

The scope of each of these functions is described below.

4.1.1 End User Access

End user access to call and service processing will be provided via the following access arrangements:

- line interfaces that are provided by radio access systems
- traditional trunk and SS7 interfaces
- other types of network access arrangements such as roamer ports

4.1.2 Service Invocation and Control

Call and service processing for WIN builds upon the call processing infrastructure of existing MSCs. It does so by using a generic model of existing call control functionality to process basic two-party calls, then adding service switching functionality to invoke and manage WIN service logic. Once invoked, WIN service logic is executed under the control of service control functionality in conjunction with service data functionality. With this distributed approach to call and service processing, the existing call control functionality retains ultimate responsibility for the integrity of calls, as well as for the control of call processing resources.

The following call and service processing constraints apply for WIN:

a). Call control and service switching functionality are tightly coupled in the MSC, thus the relationship between SSF and CCF is not standardized.

b). A call is either between two or more end users that are external to the network and addressable via a directory number or combination of directory number and bearer capability, or a call is between one or more end users and the network itself.

c). A call may be initiated by an end user, or by an SCF within the network on behalf of an end user. To supplement a call, WIN service logic may either be invoked by an end user served by a WIN MSC, or by the network on behalf of an end user.

d). A call may span multiple MSCs. As such, each MSC only controls the portion of the call in that MSC. Call processing is functionally separated between MSCs. WIN service logic invoked on WIN MSCs in such an inter-MSC call are managed independently by each WIN MSC.

e). MSCs can be viewed as having two functionally separate sets of call processing logic that coordinate call processing activities to create and maintain a basic two-party call. This functional separation is provided between the originating portion of the call and the terminating portion of the call. This functional separation should be maintained in a WIN MSC to allow WIN service logic invoked on the originating portion of the call (i.e. on behalf of the calling party) to be managed independently of WIN service logic invoked on the terminating portion of the call (i.e. on behalf of the called party).

f). It is desirable to allow multiple WIN-supported service logic instances to be simultaneously active for a given end user. It is also recognized that non-WIN service logic will continue to exist in the network. As such, service feature logic instances mechanisms for WIN should:

- determine which service logic to invoke for a given service request. This mechanism should select the appropriate WIN-supported service logic or non-WIN- supported service logic, and block the invocation of any other service logic for that particular service request;
- manage WIN- and non-WIN-supported service logic instances which are simultaneously active (this may require limiting the service logic instances which are active);
- ensure that simultaneously active WIN-supported service logic instances adhere to single-ended, single point of control service processing.

g). The distributed approach and added complexity of call and service processing for WIN requires mechanisms for fault detection and recovery, allowing graceful termination of calls and appropriate treatments for end users.

4.1.3 End User Interaction

End user interaction with the network to send and receive information is provided by service switching and call control resources, augmented by specialized resources. These specialized resources are controlled by service control functionality, and are connected to end users via call control and service switching functionality.

4.1.4 Service Management

Service management functionality is used to provision and manage the service control functionality, service data functionality, and specialized resource functionality in the network, outside of the context of call and service processing. Standardized interfaces for this functionality are outside the scope of WIN. However, the ability of a service subscriber to interact directly with subscriber-specific service management information will not be excluded or constrained for WIN.

4.2 DFP model

The following figure shows the DFP model for WIN:

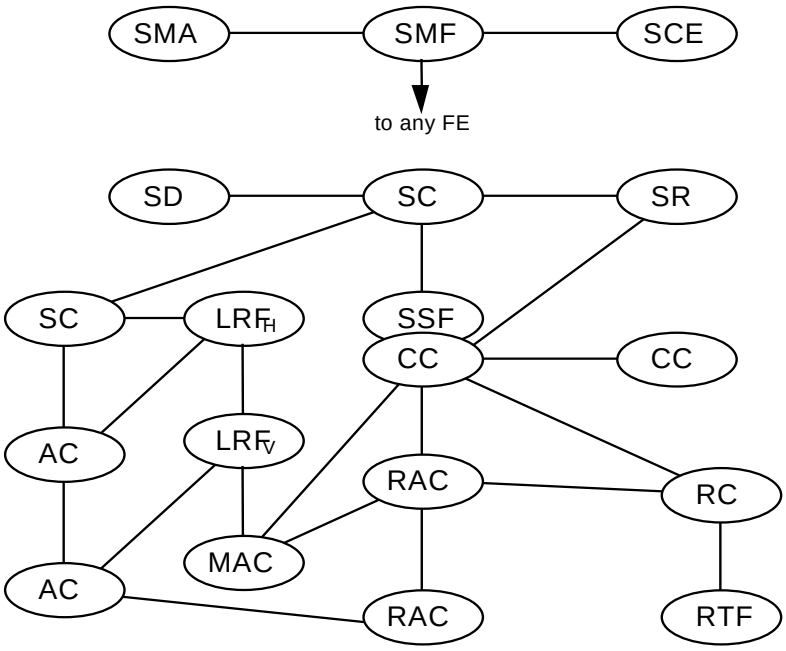

Figure 4: WIN Distributed Functional Model

Functional modeling facilitates the development of information flows between the FEs in modeling network functionality and services. This model has been developed to be non-service specific. It is a functional model and does not imply any limitations regarding physical implementations or distribution of functions to physical platforms.

4.2.1 Functional Entities

Authentication Control Function (ACF)

The Authentication Control Function (ACF) provides the service logic and service data function to provide authentication, voice privacy and signaling message encryption functions. The ACF:

a) interacts with the SCF, LRF_H, LRF_V, RACF and other ACF functional entities for the authentication of mobile stations
b) maintains the authentication parameters for the MS
c) authenticates the MS access
d) computes the voice privacy mask and signaling message encryption key for MS origination and page response accesses
e) updates the MS's authentication parameters
f) provides trigger mechanisms to access WIN service logic

Call Control Function (CCF)

The Call Control Function (CCF) provides call and service processing and control. The CCF:

a) establishes, manipulates and releases call and connection as requested by the MACF, RACF, RCF and by other CCF functional entities
b) provides the capability to associate and relate RCF functional entities, and other CCF functional entities that are involved in a particular call and/or connection instance (that may be due to SSF requests)
c) manages the relationship between RCF functional entities and between other CCF functional entities involved in a call (e.g. supervises the overall perspective of the call and connection)
d) interacts with the MACF and RACF to establish an information exchange path (e.g.,

call delivery, short message delivery) to an MS

e) provides trigger mechanisms to access WIN functionality (e.g., passes events to the SSF)

Location Registration Functions (LRF_H, LRF_V)

The Location Registration Function (LRF) provides the service logic and service data function to manage the mobility aspects for wireless users. There are two complementary LRF FEs: LRF_H and LRF_V.

The LRF_H:

a) interacts with the LRF_V and MACF(when the mobile station is in the home system) functional entities to maintain the location and active/inactive status for mobile stations
b) maintains the subscriber profile (e.g., switch-based features, triggers) and interacts with the LRF_V functional entity to transfer and update the subscriber profile
c) interacts with the LRF_V functional entity to provide a routing address for establishment of an information exchange path (e.g., call delivery, short message delivery)
d) interacts with the ACF functional entity to provide authentication, voice privacy and signaling message encryption for mobile stations.
e) maintains mobile station access information (e.g., SMS pending flag)
f) provides trigger mechanisms to access WIN service logic at an SCF

The LRF_V:

a) interacts with the LRF_H and MACF functional entities to maintain the location and active/inactive status for mobile stations
b) stores the subscriber profile (e.g., switch-based features, triggers) and interacts with the LRF_H and the MACF functional entities to transfer and update the subscriber profile;
c) interacts with the LRF_H and the MACF functional entities to provide a routing address for establishment of an information exchange path (e.g., call delivery, short message delivery);
d) interacts with the ACF functional entity to provide authentication, voice privacy and signaling message encryption for mobile stations.

e) at the request of the LRF_H functional entity, interacts with the MACF functional entity to provide mobile station notification information
f) provides trigger mechanisms to access WIN service logic at an SCF

Mobile Station Access Control Function (MACF)

The Mobile Station Access Control Function (MACF) stores subscriber data and dynamically associates system resources with a particular set of call instance data. The MACF:

a) interacts with the LRF_H (when the mobile station is in the home system), LRF_V and RACF functional entities to maintain the location and active/inactive status for mobile stations
b) stores the subscriber profile (e.g., switch-based features, triggers) and interacts with the SSF/CCF and with the LRF_V functional entities to transfer and update the subscriber profile
c) provides subscriber profile information (e.g., switch-based services, triggers) and authorization information to the CCF and RACF functional entities
d) maintains the mobile station access information (e.g., SMS pending flag)
e) interacts with the RACF and LRF_V functional entities to provide a routing address for establishment of an information exchange path (e.g., call delivery, short message delivery) to an MS
f) interacts with the RACF functional entity to establish an information exchange path (e.g., call delivery, short message delivery) to an MS
g) interacts with the RACF functional entity to verify the presence of the mobile station
h) at the request of the LRF_V functional entity, interacts with the RACF functional entity to provide mobile station notification information
i) interacts with the LRF_V functional entity to provide the paging strategy to the RACF functional entity to verify the presence of the mobile station
j) provides trigger mechanisms to access WIN service logic

RadioAccess Control Function (RACF)

The Radio Access Control Function (RACF) provides the service logic and service data functionality specifically related to the radio link. The RACF:

a) interacts with the CCF, ACF, MACF, RCF and with other RACF functional entities in the processing of call, non-call, or service related functions
b) interacts with the CCF and MACF to establish an information exchange path (e.g., call delivery, short message delivery) to an MS
c) interacts with the ACF to authenticate the MS access
d) interacts with the MACF to provide a routing address for establishment of an information exchange path (e.g., call delivery, short message delivery)
e) manages the RCF functions for associated RCFs
f) provides radio access control functions such as assignment of radio resources
g) interacts with the associated RCF and with other RACF functional entities to coordinate handoff activities, including the determination of target RCFs, handoff decision and handoff completion
h) interacts with other RACF functional entities to process border cell operations
i) contains service logic functionality to handle service requests that are specific to radio bearer requirements
j) executes mobile station paging

Radio Control Function (RCF)

The Radio Control Function (RCF) provides the radio port and radio port control. The RCF:

a) establishes, manipulates and releases call/connection as "requested" by the RACF, CCF, and RTF
b) provides radio functions including carrier generation, signal amplification, selective filtering, modulation and demodulation, radio channel assignment and supervision
c) provides interconnection between the radio and network bearer connections

Radio Terminal Function (RTF)

The Radio Terminal Function (RTF) provides access for wireless users. It is the interface between the wireless user and network call control functions. The RTF:

a) provides for user access, interacting with the user to establish, maintain, modify and release as required, a call or instance of service
b) interacts with the Radio Control Function (RCF) using service requests (e.g., setup, transfer, hold, etc.) for the establishment, manipulation and release of a call or instance of service

c) receives indications relating to the call or service from the RCF and relays them to the user as required
d) maintains call and service state information as perceived by this functional entity

Service Control Function (SCF)

The Service Control Function (SCF) commands call control functions in the processing of WIN provided and custom service requests. The SCF may interact with other functional entities to access additional logic or to obtain information (service or user data) required to process a call and service logic instance. The SCF:

a) interfaces and interacts with service switching function/call control function
b) contains the logic and processing capability required to handle WIN provided service attempts
c) interfaces and interacts with other SCFs for secured data acquisition and manipulation, distributed service control and unsolicited service notifications, if necessary
d) interfaces and interacts with SDFs for data acquisition and manipulation of data
e) interfaces and interacts with SRFs

Service Creation Entity Function (SCEF)

The Service Creation Entity Function (SCEF) provides the capability for the creation, verification, and testing of WIN services. The output of the SCEF includes service logic and service data templates.

Service Data Function (SDF)

The Service Data Function (SDF) contains customer and network data for real-time access by the SCF in the execution of WIN-provided services. The SDF interfaces and interacts with SCFs as required. The SDF contains data relating directly to the provision or operation of WIN-provided services, thus it does not necessarily encompass data provided by a third party such as credit information, but may provide access to the data.

Service Management Access Function (SMAF)

The Service Management Access Function (SMAF) provides the human interface to service management functions.

Service Management Function (SMF)

The Service Management Function (SMF) provides overall service management functionality for the network. The SMF may interact with any or all of the other FEs to perform service provisioning, monitoring, testing, and subscriber data management functions.

Service Switching Function (SSF)

The Service Switching Function (SSF) is associated with the CCF and provides the set of functions required for interaction between the CCF and a service control function (SCF). The SSF:

a) extends the logic of the CCF to include recognition of service control triggers and to interact with the SCF
b) manages signaling between the CCF and the SCF
c) modifies call and connection processing functions (in the CCF) as required to process requests for WIN provided service usage under the control of the SCF

Special Resource Function (SRF)

The Specialized Resource Function (SRF) provides the specialized resources required for the execution of WIN-provided services (e.g., digit receivers, announcements, conference bridges, etc.). The SRF:

a) interfaces and interacts with SCF and SSF (and with the CCF)
b) may contain the logic and processing capability to receive, send and convert information received from users
c) may contain functionality similar to the CCF to manage bearer connections to the specialized resources

4.3 WIN Reference Model

The following figure represents the the network entities and the associated interface reference points that may logically comprise a wireless network :

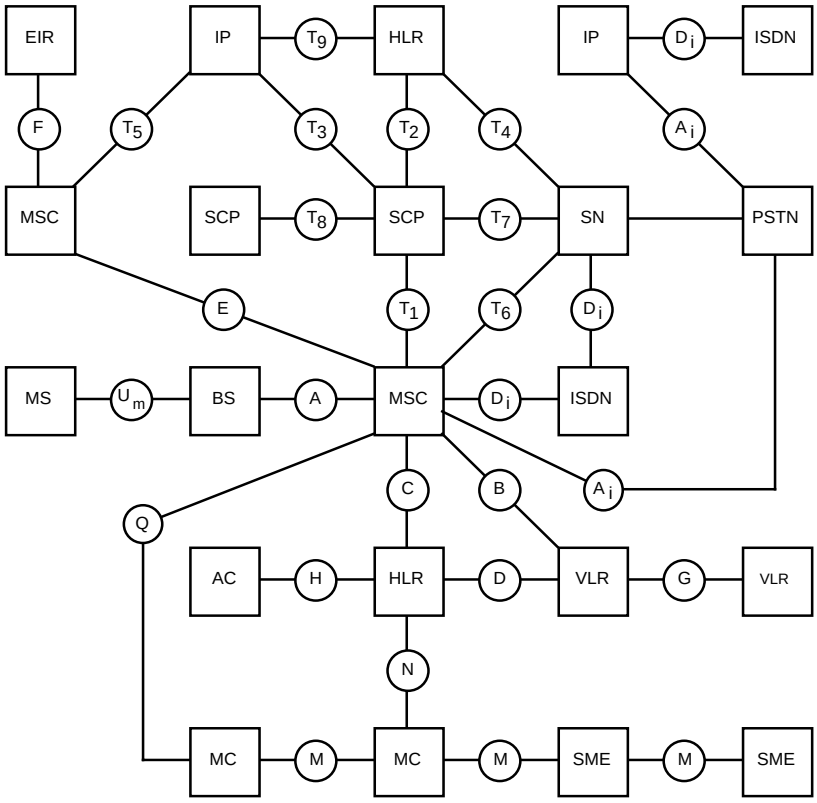

Figure 5: Network reference model.

4.3.1 Network Entities

Intelligent Peripheral (IP)

The IP is an entity that performs specialized resource functions such as playing announcements, collecting digits, performing speech-to-text or text-to-speech conversion recording and storing voice messages, facsimile services, data services, and so on.

Service Control Point (SCP)

The SCP is an entity that acts as a real-time database and transaction processing system to provide service control and service data functionality.

Service Node (SN)

The SN is an entity that provides service control, service data, specialized resources and call control functions to support bearer related services.

4.4 Call Modeling for WIN

Call modeling provides a high-level service, vendor, and implementation independent abstraction of WIN call and connection processing in the SSF and CCF. This abstraction provides an observable view of SSF/CCF activities and resources to the SCF, enabling the SCF to interact with the SSF in the course of executing service logic. To provide an observable view of the SSF/CCF to the SCF, and to enable the SCF to interact with the SSF, call modeling for WIN provides the following:

- a foundation based on the existing base of evolvable network technology;
- single-ended view of SSF/CCF call processing in terms of both Originating and Terminating Basic Call State Models (BCSMs);
- a framework for defining trigger requirements in the BCSMs to invoke WIN service logic and to report call processing events to WIN service logic in terms of Detection Points (DPs), which can be used in combinations by the implementor to provide network services;
- a framework for ensuring correct sequencing of functions within an SSF/CCF in terms of BCSM Points in Call (PICs) and transitions;
- rules of representing and handling service logic instance interactions; and
- a framework for defining the information flows (relationships) between an SSF and an SCF.

Examples of call and connection processing functions accessible to the SCF from the SSF/CCF as reflected in the WIN information flows (intersystem signaling operations) include functions to:

- influence the flow of call processing (e.g., rerouting a call, clearing a call or providing serial calling);
- access and change information related to call processing;
- manipulate the connectivity of the call;
- monitor for events related to call processing and connectivity manipulation (e.g., no answer, busy, disconnect).

4.4.1 Service Logic Processing

The modeling of service logic processing for WIN provides an abstraction of SCF activities and resources needed to support this service logic execution, as well as an abstraction of SRF and SDF activities and resources accessible to the SCF.

To provide an abstraction of SCF activities and resources, as well as SRF and SDF activities and resources accessible to the SCF, modeling of service logic processing for WIN provides the following:

- a high-level service, vendor and implementation independent abstraction of service logic processing in the SCF, specialized resources in the SRF and service data in the SDF;
- a characterization of the capabilities of an SRF and SDF made available to an SCF;
- a framework for defining the information flows (relationships) between an SRF and an SCF and between an SDF and an SCF.

The SRF, SCF, and SDF modeling only provides high-level modeling of necessary functionality, but makes no recommendations on specific mechanisms to implement this functionality (e.g., no recommendations on service logic invocation, management of service logic instance interactions, reservation and allocation of specialized resources, data architecture and access to data). The modeling primarily addresses the functionality for normal call processing scenarios.

Examples of specialized resource functions accessible to the SCF from the SRF as reflected in the related WIN information flows include functions to:

– send information to users participating in a call (e.g., prompts for information, announcements);

– receive information from users participating in a call (e.g., authorization codes);
– modify user information (e.g., text to speech synthesis, protocol conversion); and
– provide specialized connection resources (e.g., audio conference bridge, information distribution bridge).

Examples of service data processing functions accessible to the SCF from the SDF as reflected in the related WIN information flows include functions to

- access service information (e.g., subscription data parameters); and
- update service information (e.g., sum of charging).

4.4.2 WIN Basic Call State Model

The BCSM is a high-level model description of Call Control Function (CCF) activities required to establish and maintain communication paths for users. As such, it identifies a set of basic call and connection activities in a CCF and shows how these activities are joined together to process a basic call and connection (i.e. establish and maintain a communication path for a user).

Many aspects of the BCSM are not externally visible to WIN service logic instances. However, aspects of the BCSM that are reflected upward to the Service Switching Function (SSF) are visible to WIN service logic instances. The BCSM is primarily an explanatory tool for providing a representation of CCF activities that can be analyzed to determine which aspects of the BCSM will be visible to WIN service logic instances, if any, and what level of abstraction and granularity is appropriate for this visibility.

The BCSM identifies points in basic call and connection processing when WIN service logic instances are permitted to interact with basic call and connection control capabilities. In particular, it provides a framework for describing basic call and connection events that could lead to the invocation of WIN service logic instances or that should be reported to active WIN service logic instances, for describing those points in call and connection processing at which these events are detected, and for describing those points in call and connection processing when the transfer of control can occur.

The figure below shows the components that have been identified to describe a BCSM, to include: Points in Call (PICs), Detection Points (DPs), transitions and events. PICs

identify CCF activities required to complete one or more basic call and connection states of interest to WIN service logic instances. DPs indicate points in basic call and connection processing at which transfer of control can occur. Transitions indicate the normal flow of basic call and connection processing from one PIC to a DP or to another PIC. Events cause and are associated with transitions.

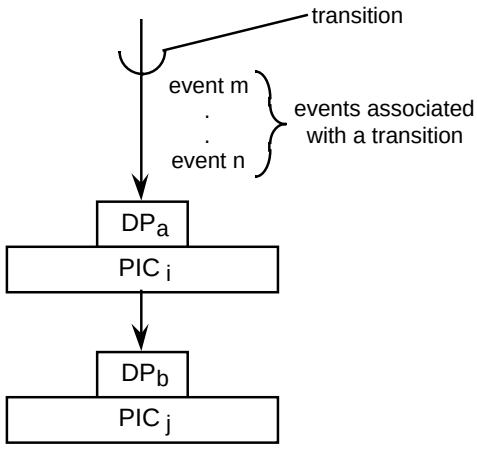

Figure 6: BCSM components

4.4.2.1 Originating BCSM

The originating half of the BCSM corresponds to that portion of the BCSM associated with the originating party (see figure 7).

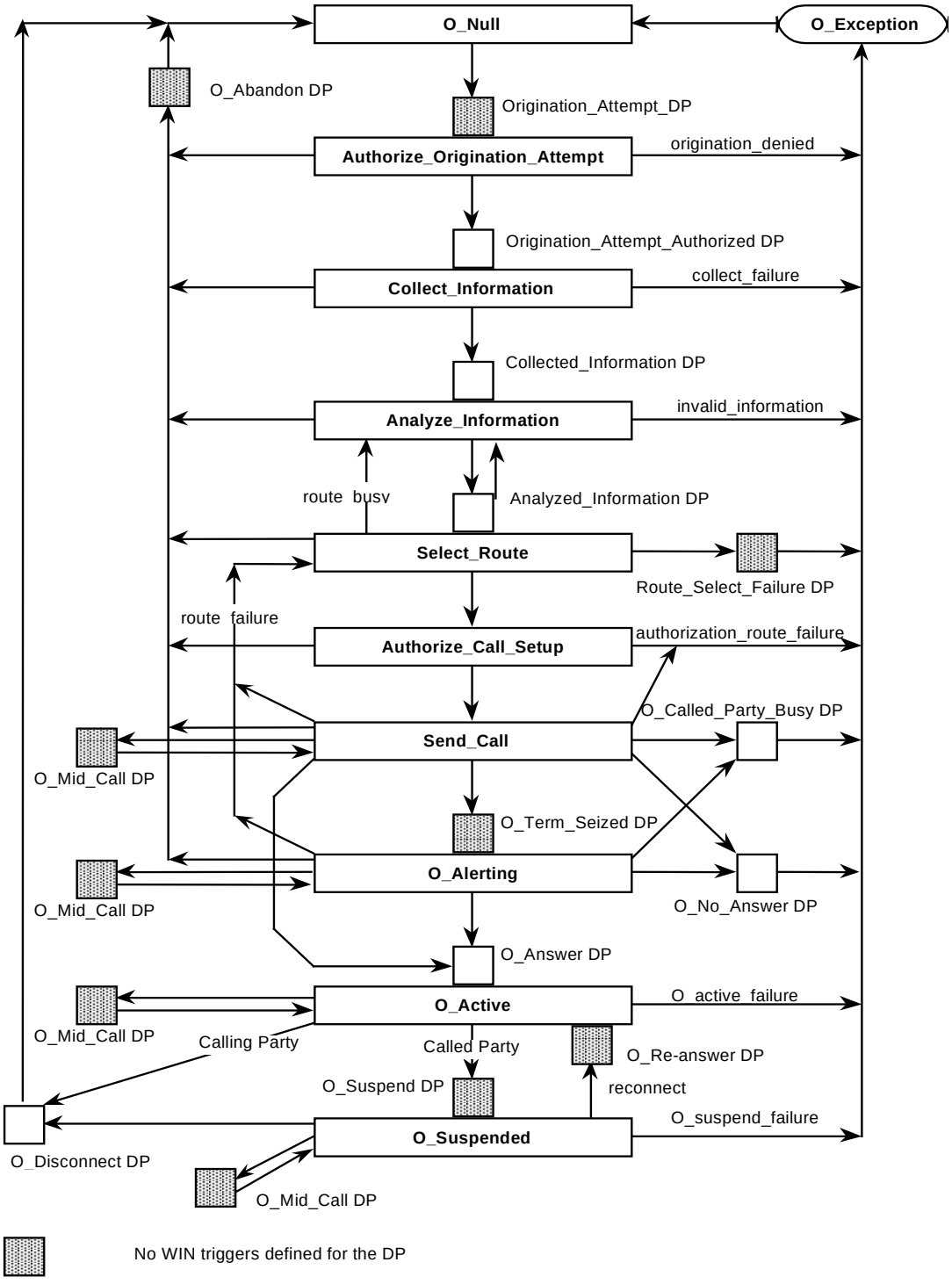

Figure 7: Originating BCSM

4.4.2.2 Terminating BCSM

The terminating half of the BCSM corresponds to that portion of the BCSM associated with the terminating party (see figure 8).

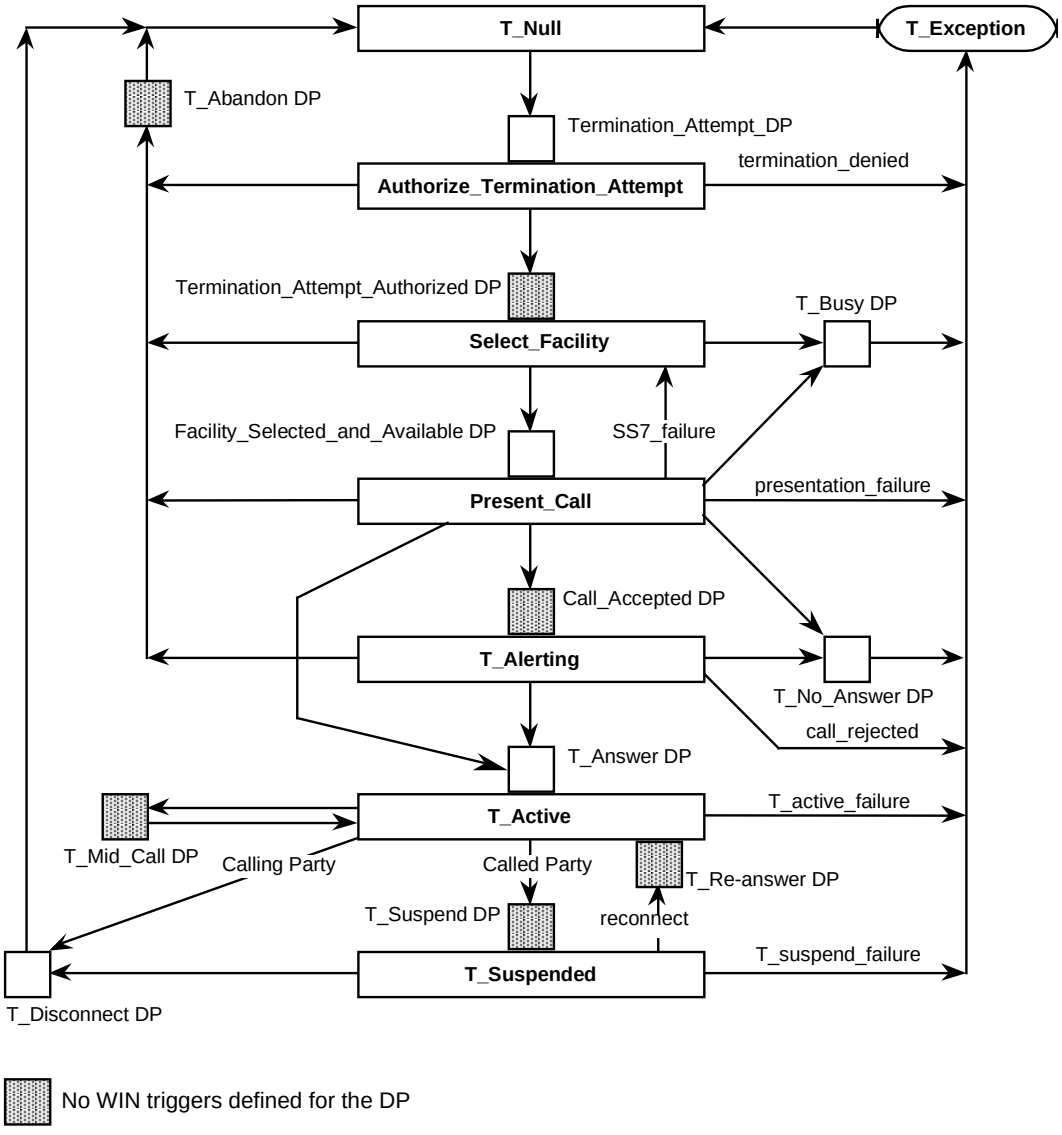

Figure 8: Terminating BCSM

4.4.3 BCSM Detection Points

Certain call and connection events may be visible to WIN service logic instances. DPs are the points in the call processing at which these events are detected.
A DP can be armed in order to notify a WIN service logic instance that the DP was encountered, and potentially to allow the WIN service logic instance to influence subsequent call processing. If a DP is not armed, the SSF/CCF continues call processing without SCF involvement.

DPs are characterized by the following four attributes:

1. Arming/disarming mechanism. A DP must be armed in order for the event to be detected. A DP may be statically armed or dynamically armed. A DP is statically armed through service feature provisioning. A statically armed DP remains armed until explicitly disarmed. Statically armed DPs are of type TDP-R or TDP-N.
   A DP may be dynamically armed by a Service Logic Program (SLP) instance at an SCF within the context of the current call and the current control relationship with that SLP instance at that SCF. Dynamically armed DPs of this type are labeled EDP-- R or EDP-N.
   While the SSF/CCF-SCF control relationship exists, the dynamically armed triggers at EDPs may be adjusted as needed by the SLP instance at the SCF. EDPs may remain armed to provide notifications only to the SLP instance at the SCF when the relationship shifts from control to monitoring. These dynamically armed EDPs are automatically disarmed when the relationship terminates, even if the call continues. If the relationship shifts to monitoring mode, a new control relationship may be established with another SLP instance at the same or a different SCF within the same call.
   When a mobile station initially registers within the serving area of an SSF/CCF, the set of DPs armed, the trigger criteria and related information (e.g., the SCF to which a call handling instruction request should be addressed) need to be placed in the SSF/CCF serving the subscriber when the registration takes place. This represents dynamic geographic placement of statically armed DPs, and is distinct from dynamic DP arming as discussed above. This requires that an image of the statically armed DPs (type TDP-R and TDP-N) for the registering subscriber be provided to the SSF/CCF as part of the registration notification process.

Upon intersystem handoff, the original SSF/CCF becomes the anchor SSF/CCF and remains responsible for the relationship(s) to the SCF(s) influencing the call. Therefore, there is no impact as a result of the handoff.

Specific triggers may be dynamically armed as TDPs within the context of the current call. The SCF response to the SSF/CCF can provide this trigger arming information.

2. Criteria. In addition to the condition that a DP be armed, DP criteria must be satisfied in order to notify the SCF that the DP was encountered.
3. Relationship. Given that an armed DP was encountered and DP criteria are satisfied, the SSF may provide an information flow via a relationship:
   a) If this relationship is between the SSF/CCF and the SCF for the purpose of call and service logic processing, it is considered to be a WIN service relationship. This relationship may be of two types:
      - a control relationship if the SCF is able to influence call processing via the relationship
      - a monitor relationship if the SCF is not able to influence call processing via the relationship
   b) If this relationship is between the SSF/CCF and the SCF or the SMF for management purposes, it is considered to be a service management control relationship.

4. Call processing suspension. Given that an armed DP was encountered and DP criteria are satisfied for a WIN service control relationship, the SSF may suspend call processing to allow the SCF to influence subsequent call processing. When call processing is suspended, the SSF sends an information flow to the SCF requesting instructions, and waits for a response. When call processing is not suspended, the SSF sends an information flow notifying the SCF that a DP was encountered, and does not expect a response. This attribute is set by the same mechanism that arms the DP.

Based on these attributes, four types of DPs are identified for WIN. The DP types are:

1. Trigger Detection Point – Request (TDP-R)
2. Trigger Detection Point – Notification (TDP-N)
3. Event Detection Point – Request (EDP-R)
4. Event Detection Point – Notification (EDP-N)

A Trigger Detection Point (TDP) is statically or dynamically armed. Each TDP is associated with specific criteria. When a TDP-R is detected, a query is launched to the SCF to initiate a control relationship between the SSF/CCF and the SCF. No further TDP-Rs may be processed while this relationship continues and remains as a control relationship. When a TDP-N is detected, a single message notification is launched to the SCF outside the context of any existing relationship. When a TDP-R is detected, call processing can be suspended. A TDP-N cannot suspend call processing.

An Event Detection Point (EDP) is dynamically armed in the context of an existing control relationship between the SSF/CCF and the SCF. EDPs are not associated with specific criteria. When an EDP-R is detected, a query is launched to the SCF within the context of the existing control relationship between SSF/CCF and SCF. When an EDP-N is detected, a single message notification is launched to the SCF as part of a control or monitor relationship between the SSF/CCF and the SCF. When an EDP-R is detected, call processing can be suspended. EDP-Ns cannot suspend call processing. When TDP-R and all EDP-R processing is completed, but there remain armed EDP-Ns, the relationship between the SSF/CCF and the SCF transitions to a monitoring relationship. This relationship may not transition back to a control relationship. When the relationship between the SSF/CCF and the SCF is terminated, any remaining EDP-Rs or EDP-Ns are deleted since they are meaningful only within the SSF/CCF-SCF relationship in which they were armed.

4.4.3.1 Detection Points Processing

DP processing rules include service and feature interaction management rules.
DP processing involves:

1. traffic management actions (call gapping and service filtering – not subject to standardization at this time)
2. determining if DP criteria are satisfied
3. handling service logic instance interactions when invoking new instances of WIN and non-WIN service logic
4. formulating information flows to send to one or more SCFs

If a DP is armed, it may be armed as a TDP, as an EDP, or as both a TDP and an EDP for the same instance of a BCSM. The SSF/CCF shall apply the following set of rules during DP criteria processing to ensure a single point of control:

Rule 1: At any DP, a specific trigger condition can only trigger one service logic program instance (SLPI) at a time. The SSF shall act on one trigger at a time, even if multiple triggers are detected at a DP.

Rule 2: At any DP, processing of notification type DPs (EDP-N and TDP-N) has higher priority than processing of request type DPs (EDP-R and TDP-R).

Rule 3: If a DP is both armed as EDP and TDP, then the EDP processing has higher priority than the TDP processing since the EDP has been armed in an already existing SSF-SCF relationship.

Rule 4: If a DP is both armed as EDP-R and TDP-R, The EDP-R is processed first and, if the control relationship is terminated as a result of the EDP-R processing, processing of the TDP-R is allowed.

In summary, the SSF processes DPs in the following priority order:

Highest priority:	EDP-N
	TDP-N
	EDP-R
Lowest priority:	TDP-R

If a TDP-R or EDP-R is detected, the SSF shall formulate and send a request message to a SCF, start a timer and wait for a response from the SCF prior to resumption of call processing by the CCF.

If a TDP-N or EDP-N is detected, the SSF shall formulate and send a notification message to an SCF.

TDP-N criteria may be processed whether or not there is an existing control relationship for the same portion of the call, since a TDP-N does not open a control relationship. This procedure has no effect on the existing control relationship.

4.4.4 Triggers

Triggers must be one of three categories:

1. Subscriber-based. If a trigger is subscriber-based, only calls involving the subscriber (mobile station or user) can encounter the trigger. Subscriber-based criteria are sent from the HLR to the Serving MSC as the subscriber roams.
2. Group-based. If a trigger is group-based, only calls involving a member of the group (mobile station or user) can encounter the trigger. Group-based trigger criteria may be sent from the HLR to the Serving MSC (similar to the subscriber-based criteria), or may reside as static data in the MSC (similar to office-based criteria).
3. Office-based. If a trigger is office-based, then any call that satisfies the DP criteria can encounter the trigger. Office-based trigger criteria reside as static data in the MSC.

A WIN trigger occurs when all of the following conditions are satisfied:

1. The CCF is processing a call and encounters a Trigger Detection Point
2. The trigger is active and armed
   - if the trigger is subscriber-based, the call must be originating or terminating with the subscriber for the trigger to be active
   - if the trigger is group-based, the call must be originating or terminating with a member of the group for the trigger to be active
   - if the trigger is office based, the trigger is active for all calls
3. Appropriate trigger criteria are stored at the MSC
4. The information available at the MSC satisfies the trigger criteria

WIN triggers may occur in the Originating BCSM or Terminating BCSM. When a trigger occurs, the MSC typically launches an *TIA/EIA-41* query to another network entity (e.g., SCP) in order to obtain the information needed to continue processing the call. Triggers can be active for various types of interfaces: trunk, line (radio port) or roamer port.

After detecting a trigger and sending a query to an SCP, the MSC receives a response indicating how to process the call. Subsequent call processing may lead to other triggers. To protect switch and network resources from possible infinite looping, the MSC shall terminate (i.e., apply final treatment to) any call that encounters more triggers than the value of MaximumSerialTriggers without routing out of the same MSC. MaximumSerialTriggers shall be administered by the network operator with a default, office-wide value of 6.

4.4.4.1 Trigger Profile

Information	Usage
DP	Identifies the BCSM DP to be armed
Trigger Type	Denotes the class of events of interest (e.g. Specific_Called_Party_Digit_String); some DPs have multiple trigger types, others only one
Criteria	The conditions that must be satisfied in order to notify the SCF that the DP was encountered ; may be "unconditional"
DP Type	TDP-R (SCF response is required, call processing is suspended) TDP-N (notification only, call processing is not suspended)
SCF Address	The address to which the information flow will be sent

Table 1: Information Contained in Trigger Profile

The information contained in the trigger profile is shown in Table 1. When a mobile station initially registers within the serving area of an SSF/CCF or at other times, the set of DPs armed, the trigger criteria and related trigger profile information need to be placed in the SSF/CCF serving the subscriber.

5. WIN in 3G

The Wireless Intelligent Network – Service Switching Point (WIN-SSP) is introduced to provide WIN capable services in 3G All-IP network which enable a rapid deployment of new services and a flexible control of existing services.

WIN-SSP allows the provisioning of WIN services in the CPS, which functions as an SSP and communicates, with a SCP by using the WIN protocol. One of the services to be implemented is Pre-paid Charging (PPC).

The following figure describes the relevant network entities and the interfaces for the WIN subscribers in All-IP Network environment.

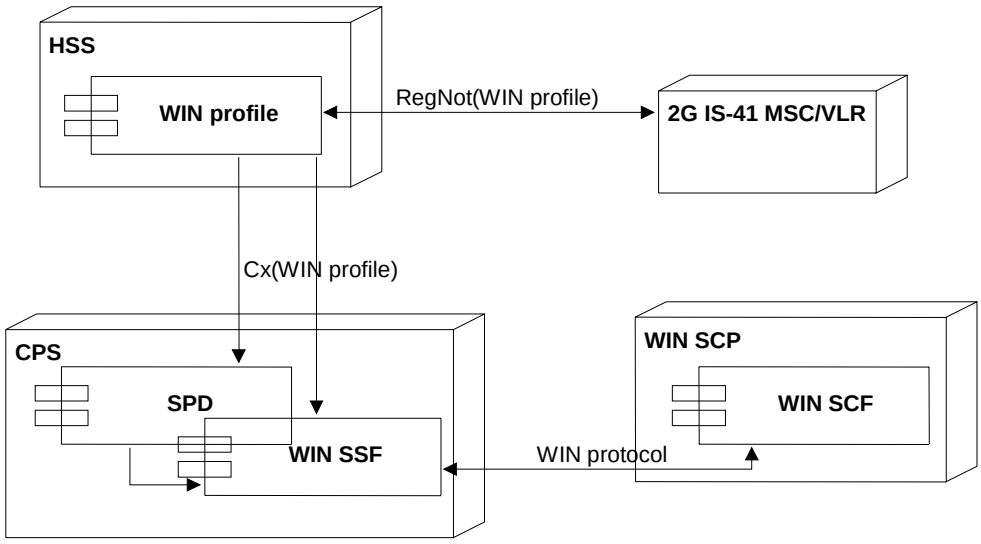

Figure 9: Architecture for WIN subscribers in All-IP Network

The WIN profile information is included in the subscriber information in location update and HSS enquiry messages. Updating of a subscriber's WIN and CAMEL service profile information is also possible in case when IN service is changed while the subscriber is roaming in 3G.

WIN profile includes the following messages:

- Send Routing Information
- Update Location

- Insert Subscriber Data

5.1 Usage of Call Model

MS to MS Calls served by the same CPS

The following figure illustrates the usage of call model for the scenario where both the calling and called parties are MSs that are local to the Originating CPS.

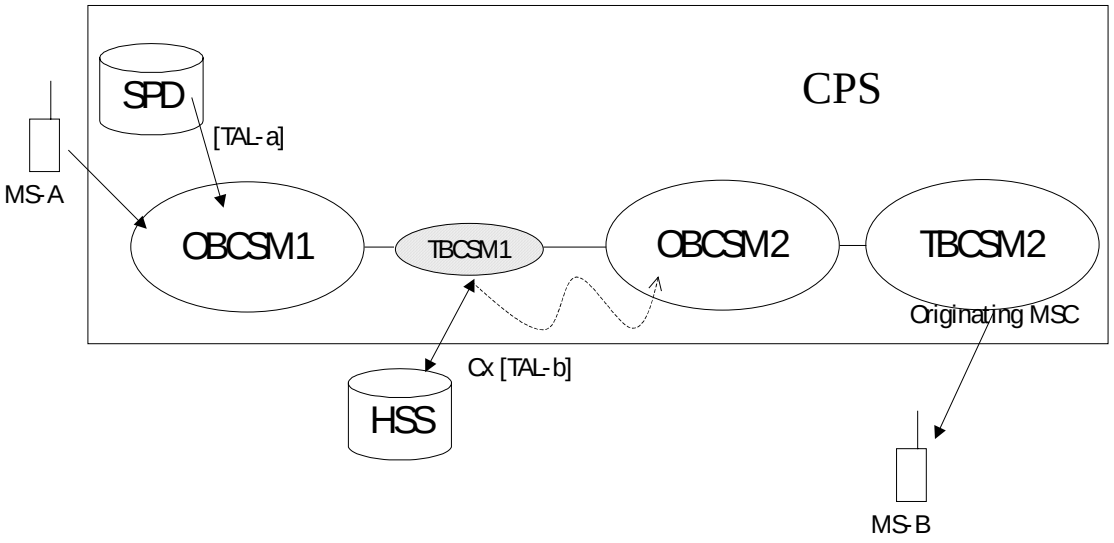

Figure 10: MS to MS Call served by the same CPS

IS41 uses two BCSMs (OBCSM1 for MS-A and TBCSM1 for MS-B) in the MS to MS local call based on the fact that the IS41 HLR has knowledge of the originating MS and terminating MS belonging to the same CPS.

- OBCSM 1 is used to support the originating party including the triggers armed on behalf of MS A.
- TBCSM 1 is used to support the terminating party including the triggers armed on behalf of MS B.

In 3G All-IP case, the HSS does not know whether MS A and MS B are served by the same CPS switch or not, so MS B is always treated as a roaming subscriber. Therefore the WIN MS to MS local call will use the existing usage of call model suggested in FN1214 .

Four BCSMs are involved in the above processing:

- OBCSM 1 (O-1) is used to support the originating party including the triggers armed on behalf of MS A.

- OBCSM 1 (O-1) is armed by the trigger stored in the SPD. This trigger is received during initial registration (i.e., Location Update). Trigger may occur depending on trigger criteria in each DP. If trigger criteria is met, then a WIN operation associated with a trigger is launched to request service from the SCP. If a TAL is returned from the SCP, it replaces the existing triggers in O-1 except office based triggers.

- TBCSM 1 (T-1) acts a proxy BCSM alias gateway BCSM, which is used to instantiate OBCSM 2 to support the roaming subscriber.

- During the terminating processing in TBCSM 1 (T-1), TAL is downloaded from the HSS via SRI to SPD at Authorize_Termination_Attempt PIC. Also TAL may be downloaded from the SCP depending on trigger criteria at the Termination_Attempt_Authorized DP. Please note that TAL downloaded either from the HSS or the SCP, which will replace the existing forward triggers but not backward triggers e.g. TAL in O-1 remains intact; only triggers after Termination_Attempt DP are affected. An OBCM 2 (O-2) is instantiated and TAL associated with O-2 is carried over after Termination_Attempt DP.

- If terminating triggers received from SCP, they will be kept in T-1 and not be carried over to T-2, but the originating triggers will be carried over to O-2.

- OBCSM 2 (O-2) is used to support the roaming party. It also handles any originating triggers that may be armed on behalf of the roaming subscriber. The issue regarding TAL associated with T-2 whether it is carried over or not is still an open issue.

- TBCSM 2 (T-2) is used to support the terminating party including the TAL read from SPD, in which the triggers armed on behalf of MS B.

Intersystem CPS to CPS Call

The following figure illustrates the usage of call model for the scenario where the calling party is an MS that is local to the Originating CPS 1 and the called MS is currently roaming in another serving CPS 2.

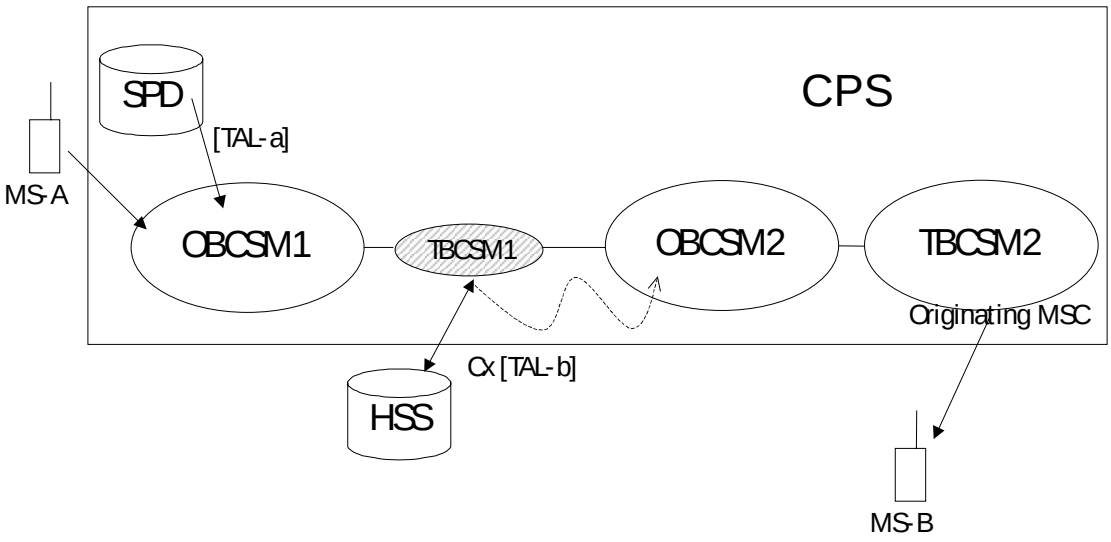

Figure 11: Intersystem CPS to CPS Call

Four BCSMs are involved in the Originating CPS:

- OBCSM 1 is used to support the originating party including the triggers armed on behalf of MS A.
- TBCSM 1 is used to support the terminating party including the triggers armed on behalf of MS B.
- OBCSM 2 is used to support the extended call from the Originating CPS 1 to the appropriate destination to reach MS B. It also handles any originating triggers that may be armed on behalf of MS B.
- TBCSM 2 is used to support the terminating processing associated with call set up via the outgoing intersystem trunk.

Intersystem CPS to IS41 Call

The following figure illustrates the usage of call model for the scenario where the calling party is an MS that is local to the Originating MSC/CPS and the called MS is currently roaming in another serving MSC/IS41.

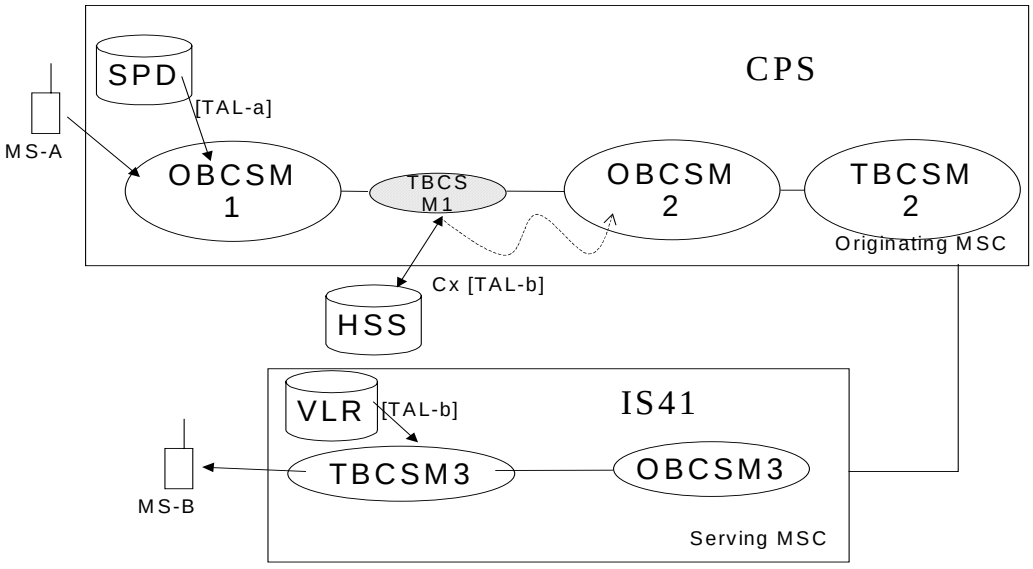

Figure 12: Intersystem CPS to IS41 Call

Four BCSMs are involved in the Originating MSC:

- OBCSM 1 is used to support the originating party including the triggers armed on behalf of MS A.
- TBCSM 1 is used to support the terminating party including the triggers armed on behalf of MS B.
- OBCSM 2 is used to support the extended call from the Originating MSC/CPS to the appropriate destination (i.e. to a TLDN in this case) to reach MS 2. It also handles any originating triggers that may be armed on behalf of MS B.
- TBCSM 2 is used to support the terminating processing associated with call set up via the outgoing intersystem trunk.

5.2 Pre-paid Charging

Pre-paid Charging (PPC) allows the subscriber to pay for voice telecommunication services prior to usage.

A PPC subscriber establishes an account with the service provider to access voice telecommunications services in home and roaming networks. Charges for voice telecommunication services are applied to the PPC account by decrementing the account in real time. The PPC subscriber may be notified about the account information at the beginning, during, or at the end of the voice telecommunications service depending on our SRF capabilities. When the account balance is low the subscriber may be notified so that the subscriber may refill the account. When the account balance is below a pre-defined threshold, the subscriber's use of voice telecommunications services may be de-authorized.

The following scenarios describe the interaction between network entities in various situations related to WIN subscriber and Pre-Paid Charging for WIN applications.

5.2.1 Call Delivery: Local Termination

This scenario describes PPC invocation upon Call Delivery. The call is terminated at the Originating MSC.

Two cases are defined, (1) Service Node (SN) based or (2) Intelligent Peripheral (IP) based. From the MSC point of view, the WIN interaction is the same for both cases.

The following figure shows the interaction between SN and MSC. Calling MS disconnects first.

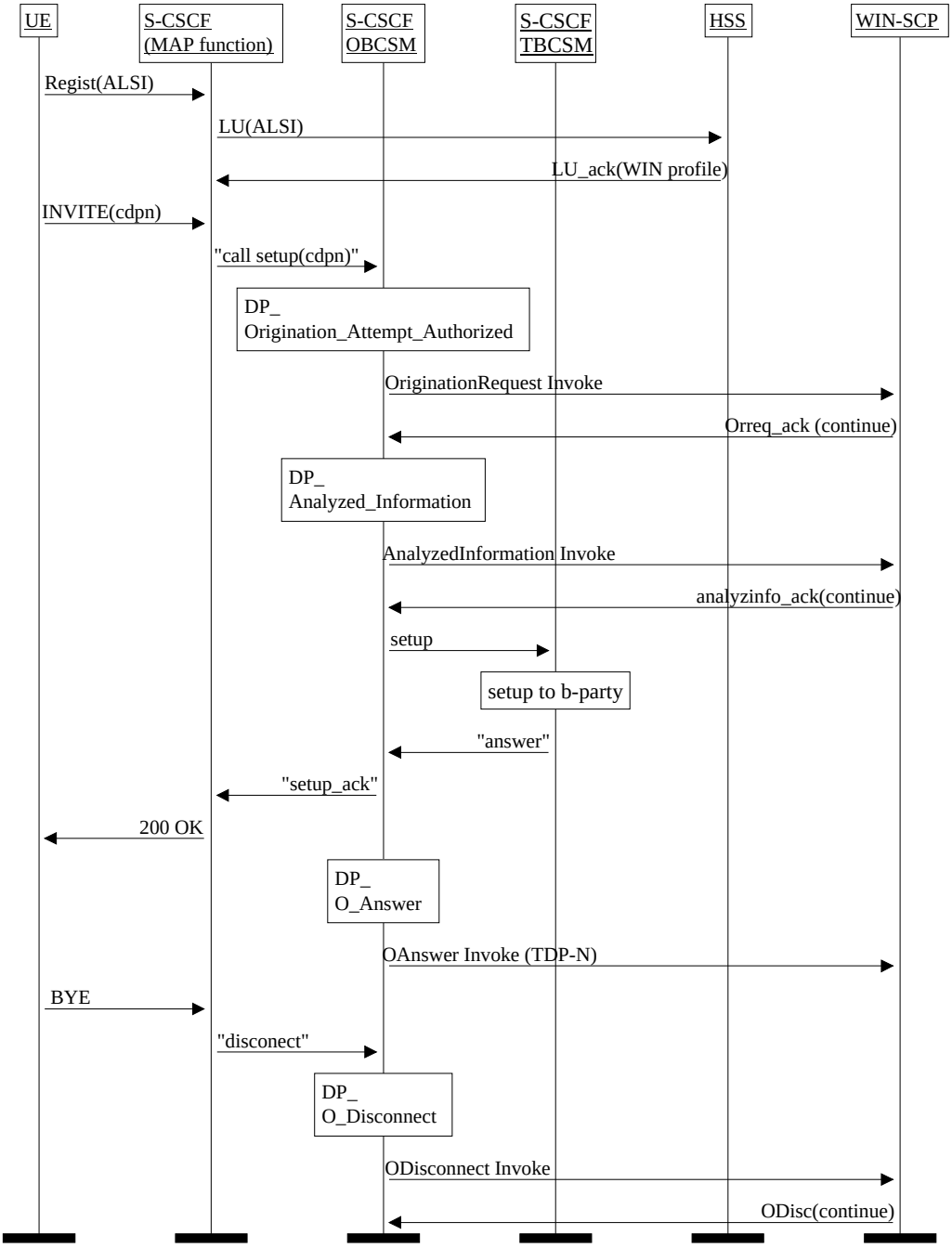

Figure 13: Call Delivery: Local Termination

5.2.2 Call Delivery: Intersystem Termination

This scenario describes PPC invocation upon Call Delivery with intersystem termination

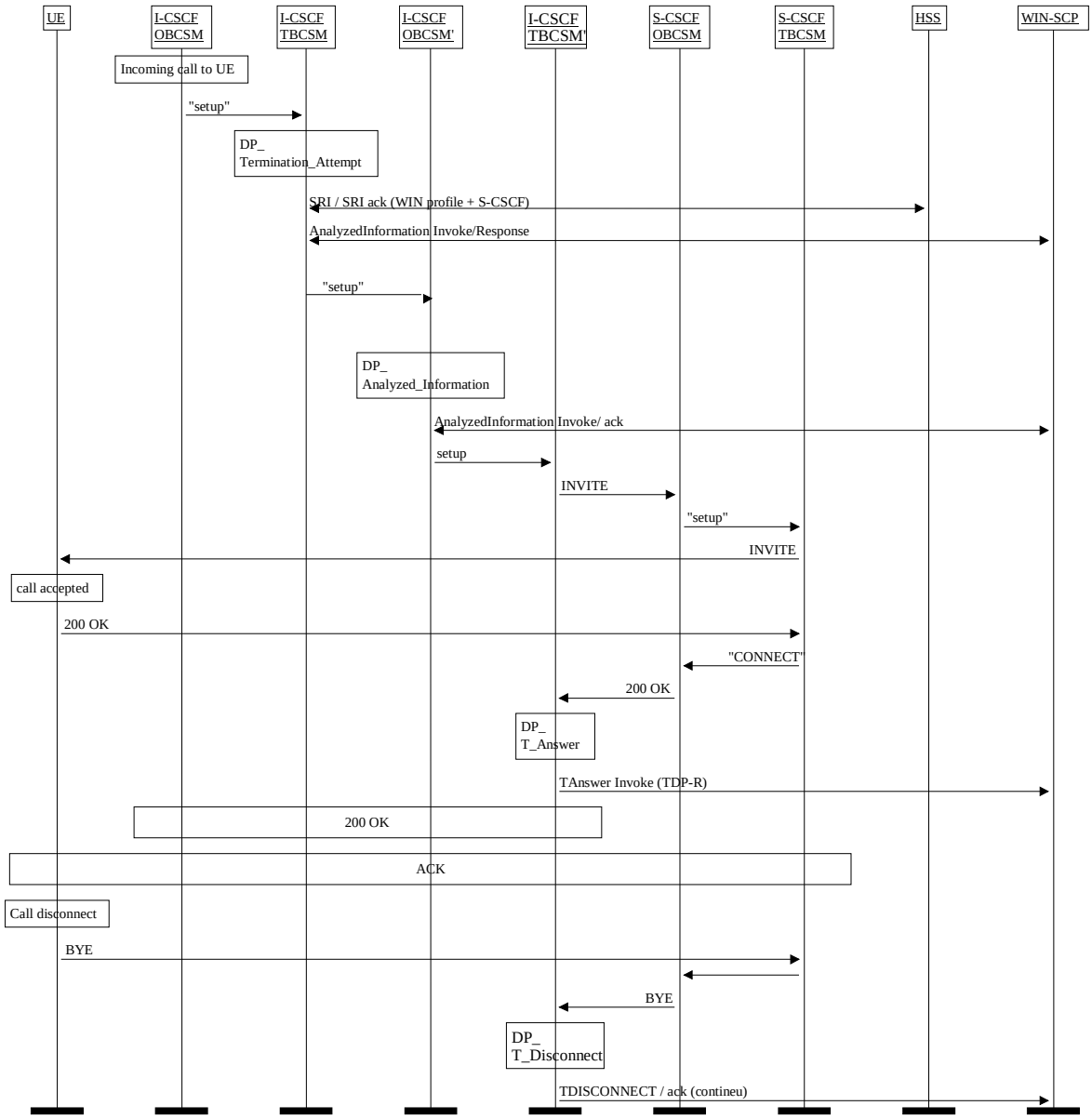

Figure 14: Call Delivery: Intersystem Termination

WIN uses the MSRN or TLDN for charging. In 3G, destination is addressed with IP address or logical name so it is not possible with the current WIN protocol to indicate IP node to SCP for charging.

5.3 Implementation architecture

The following figure shows the WIN-SSP implementation overview using current IN protocol stack.

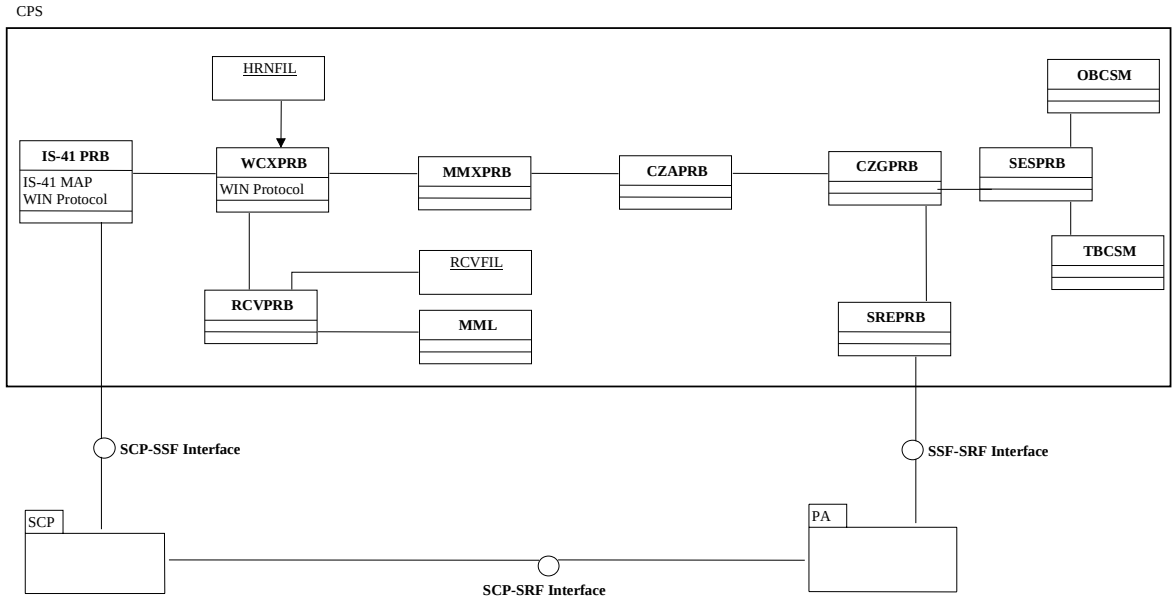

Figure 15: WIN SSP implementation architecture

5.3.1 WCXPRB

This program block has several tasks in which it would need to perform. These are to fill in generic information for the WIN protocol, generate BillingID, transform WIN messages to internal message, internal messages to WIN message, and send information to the RCVPRB for system recovery of PPC callers.

Master Process

The master process is going to do several items: have a index of BillingIDs so when a message comes in from the SCP the correct hand would be notified, generate the BillingID and Electronic Serial Number for the call, direct the UnreliableCallData message to the RCVPRB, will forward to a hand a request to send the BulkDisconnect message, and directing of the CCDIR to the correct WCX PRB.

The BillingIDs will be generated in the WCXPRB master and be stored in a table. The BillingID will be created from a sequential number generated by the master and the computer unit ID. The BillingID will be used to cross reference to get the PID of the hand so the correct hand can be given the message.

When the CCDIR is received from the SCP the correct computer unit may have not received it. The master will examine the BillingID to extract the computer unit and send the CCDIR to the correct computer unit that has WCXPRB.

When WCX PRB receives the UnreliableCallData from the SCP, the master will create a hand to handle this message. The hand will then forward this message and wait for the RCVPRB to respond. Additional information will be discussed in Hand One.

Hand One

Hand one is going to handle request from CC and SCP for a WIN operations. WCX will have to store and update information given to it from CC in and the SCP all tasks could be performed for the WIN to internal interface translation. The translation would consist of taking internal messages from the SSF and transforming them to WIN operations on a 1:1 bases. In practice this means that internal messages from the SSF to SCP will have to be modified to accommodate additional information needed by the WIN protocol. Three internal messages have been identified for modication and they are IDP, ERB, and RRB.

An alternative would be to use existing messages and any additional information that would be needed for that WIN operation would be sent in an additional message. This

option seems might cause confusion in the program blocks and will definitely put a greater load on the message bus.

This is not the case for message that are originated from the SCP. Most WIN messages from the SCP will have to be broken into multiple internal messages. This is based upon what parameters are present in the WIN operation and what our SSF supports.

In the case of UnreliableCallData is received, a message indicating this will be sent to RCVPRB. Hand one will then wait for call data for that SCP that sent the UnreliableCallData message. Hand One will then format the message CallRecoveryReport and send it to the SCP. This will possible occur multiple times until all call data is transferred to the SCP. After all information has been transferred, then the RCVPRB will send an message indicating this, when hand one will prepare a UnreliableCallData RETURN RESULT message to the SCP.

When a BulkDisconnect message is sent from the RCVPRB, the message will be sent to the correct SCP. When the SCP sends the BulkDisconnect RETURN RESULT this will be forwarded to the RCVPRB.

Hand one will as be required to send a message to the RCVPRB each time a dialog is start telling which SCP is being talked to. This will be used later in the case of a MSC failure as mentioned before in the WCX master process. Also upon termination of a dialog with the SCP a message to the RCVPRB will be sent to indicate hat the dialog has ended.

5.3.2 RCVPRB

This process is mainly for call recovery for PPC users. This takes into account of a MSC or SCP failure. This process will manage the RCVFIL by storing SCP data and call data in the case of a SCP failure, and a MML co-process. The process will consist of a master and one hand.

Master Process

The master process is mainly used for storing data to the RCVFIL and maintaining its itegrity. Upon start up the hand one will be started.

The storing of call data is necessary for fault tolerance in the system for SCP and CPS failures mainly concerned with PPC subscribers. The storing of call information for terminated call is required when the SCP does not positively acknowledge a T_Disconnect or O_Disconnect operation. When this occurs it is a sign to the CPS that there is a problem with the SCP. The CPS would store the call disconnect information in the RCVFIL file. This hand would maintain this information in the RCVFIL using a 30 minute sliding window.

When the SCP sends the UnreliableCallData message to the CPS and is received by the WCX process, the master will forward the message to this hand. The hand will then examine the RCVFIL based on the SCP MSCID number for all call related to that SCP. One or multiple CallRecoveryReport message would be sent to the SCP and acknowledged by such. This is done until all call data is sent to the SCP. Hand two will also be responsible to removing the call data from the RCVFIL upon acknowledgement from the SCP. After all data is sent the hand will send the UnreliableCallData RETURN RESULT to the SCP to terminate the dialogue.

Upon starting a dialog with an SCP, the WCXPRB will send which SCP a dialog has been started. RCVPRB will increase a counter in the RCVPRB file. When the dialog has ended the WCXPRB will send an message indicating this fact. The RCVPRB will then decrement the counter associated with this SCP.

Hand One

The MML is needed for PPC when the MSC has a major failure i.e. the switch losses power, shuts down, or restarts. Upon restart of the MSC, a procedure will need to implemented so the operator will be instructed to use the MML to say at what time did the MSC fail. The hand will then read the RCVFIL for the SCPs that were being used, i.e. the counter was greater than zero. For each SCP a message will be sent to a WCXPRB master process to send the BulkDisconnect to the SCP. After sending this

message the hand will wait for the BulkDisconnect RETURN RESULT message indication before clearing the SCP information.

5.4 Pre-paid Callers Accounts Recovery

5.4.1 Bulk Disconnection procedure

This procedure is used in case of PPC account recovery after an SSP failure. When a major SSP failure occurs, all calls are dropped. When the SSP recovers from the failure, it can inform all SCPs that were controlling PPC calls of the time the failure occurred. This information allows SCPs to update subscriber accounts based on the time a call was ended because of SSP failure.

After a failure, the SSP can recover the addresses of SCPs controlling PPC calls at the SSP, specifically SCPs associated with *T_Disconnect* and *O_Disconnect* triggers. The amount of data stored by the SSP is a configurable size sliding window (e.g., 30 minutes).

This mechanism addresses the issue of *runaway charging* for calls which have ended but for which the PPC SLP has not received disconnection information. The PPC SLP is notified that the SSP has failed and the time the failure occurred. This enables the PPC SLP to initiate internal algorithms to identify and adjust all PPC accounts for calls served by that SSP, which were active at the time of the SSP failure.

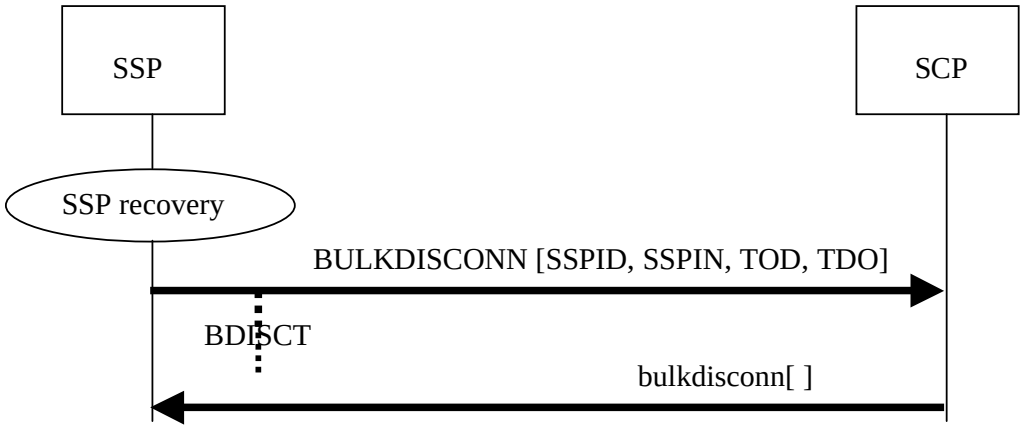

Figure 16: Bulk Desconnection procedure

After failure occurs, SSP recovers from it.
Then SSP sends BULKDISCONN to the SCP showing that all call have been dropped. The parameters are:

SSPID – Identity of the SSP
SSPIN – SSP identification number
TOD – Time Of Day, the time of day when failure occured
TDO – Time Date Offset, the time offset of Local Civil Time when failure occurred

The SCP returns an empty bulkdisconn[] (BulkDisconnect RETURN RESULT). The SCP updates PPC subscriber accounts for calls that were active at the SSP at the time the failure occurred.

Practically it meant to be so that when the major SSP failure occurs, the operator is instructed to use MML to inform when did the SSP fail. Then the RCVFIL file will be examined for any SCP that is being used. For each SCP found the BulkDisconnect message will be sent to WCXPRB with TimeOfDay and TimeOffset. Then WCXPRB will then read the HRNFIL to get SSPIN and SSPID.
After that WCXPRB will start the timer BDISCT (Bulk Disconnection Timer) with the default time,and then forward the BulkDisconnect message to the SCP (using ap_operation_s message) . When the BulkDisconnect RETURN RESULT is sent by SCP, the WCXPRB will forward it to the RCVPRB.
If timer BDISCT expires or RETURN ERROR or REJECT is received, RCVPRB will log the error.

5.4.2 UnreliableCallData procedure

This procedure is used in case of SCP failure. The storing of information about the call is requireed when SCP doesn't positively acknowledge *T_Disconnect* or *O_Disconnect* operation.When SCP recovers from failure, it sends the UnreliableCallData to the CPS (WCXPRB). The WCXPRB then will forward this message to RCVPRB. RCVPRB will examine the RCVFIL file for all call related to SCP that experienced the failure. According to this, the various number of CallRecoveryReport messages would be sent

to WCXPRB, which will forward those messages to SCP. The parameter of the CallRecoveryReport is CallRecoveryIDList, which is the list of call IDs related to the SCP. The CallRecoveryID parameter set consists of BillingID, TimeDateOffset and TimeOfDay.

After all the call information has beed sent, the RCVPRB will send the UnreliableCallData RETURN RESULT message to WCXPRB, which will forward this message to the SCP.

During SCP network entity failure, SCP failure or network failure, PPC subscriber call data is not received from the SSP. The SCP may not receive information about calls that ended during the failure period. To be able to adjust the subscriber's account, it is necessary for the SCP to obtain information on the calls that ended during the failure. The SSP may store data for calls for which it did not receive a response to a query for a calling party or called party disconnect. When the SCP recovers from a failure, it can request data from the SSP about the status of calls that were being served at that MSC. The SSP returns a list of data for calls that ended during the SCP failure.

After a failure, the SCP can recover data (stored at the SCP network entity) about calls that were active at the time the failure occurred. This data includes:

- SSP where the call was active,
- call reference (Billing ID or subscriber information identifying the call),
- start time of the call.

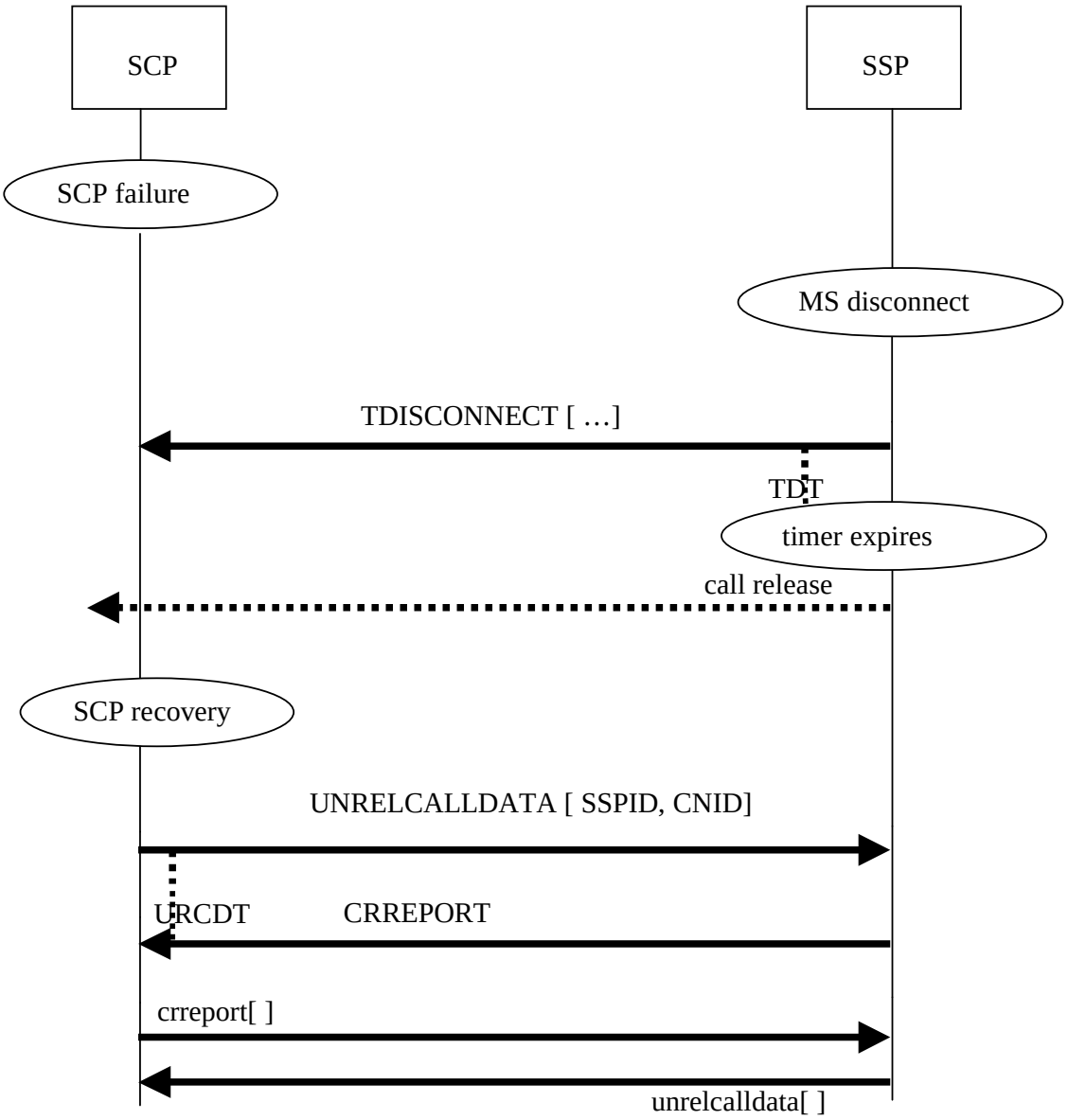

Figure 17: UnreliableCallData procedure

1. The SCP fails.
2. The call is ended by MS.
3. SSP detects the *T_Disconnect* trigger and sends a `TDISCONNECT` to the SCP associated
   with this trigger. The parameters are :

   - SCPID : Serving SCP ID
   - MSID : Served MS MSID.

- MDN : Mobile directory number. Include if available.
- BILLID : BillingID. Used to relate queries for this call.

- TRIGTYPE : Indicates the trigger encountered.
- RELCAUSE : Call release cause.
- TOD : TimeOfDay. The time of call disconnect (UTC).
- TDO : TimeDateOffset. The time offset of local civil time.

The SCP doesn't detect the message

4. The Serving SSP does not receive a `tdisconnect` and an SSP timer expires. The Serving SSP records data for the call with the MS's CNID value.

5. The Sereving SSP releases the call.

6. The SCP recovers from the failure. The SCF recovers data about SSPs handling PPC calls for subscribers served by the SCF. The SCF also recovers data related to PPC calls that started before the failure occurred.

7. The SCP sends an `UNRELCALLDATA` to the Serving SSP. The SCP's CNID parameter value is used to correlate the request to call data pertaining to recovery of the SCP failure.

8. The SSP compiles a list of stored call data that matches the received CNID value and for which no response was received to a `TDISCONNECT` or `ODISCONNECT` message. The SSP includes the time each of the calls ended. The SSP sends the requested information to the SCP in the `CRREPORT`.
   The CRIDLIST parameter represents the list of calls ended and not acknowledged in SSP.

9. SCP sends the `crreport`.
   The Serving SSP may delete the call data received by the SCF. If the scan is incomplete, the SSP sends more call data. Steps 8-9 are repeated until all the call data associated with the SCP is transmitted.

10. The Serving SSP confirms that all the call data associated with the SSP has been sent. The SSP sends an empty `unrelcalldata` to the SCP.

It's possible to have another SCP failure during the failure recovery. During a failure, PPC subscriber call data is not received from the SSP. The SCP may not receive information about calls that ended during the failure period. To be able to adjust the subscriber's account, it is necessary for the SCP to obtain information on the calls that ended during the failure.

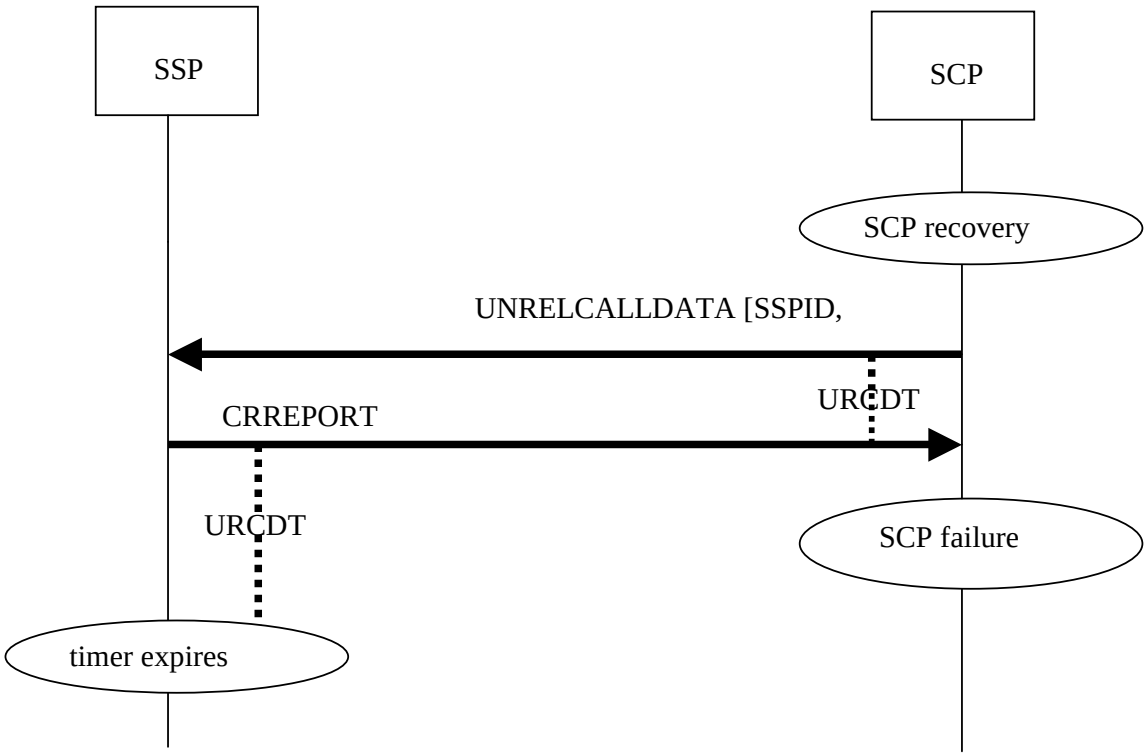

Figure 18: UnreliableCallData: SCP failure during failure recoivery

1. The SCP recovers from a failure. The SCF recovers data about MSCs handling PPC calls for subscribers served by the SCF. The SCF also recovers data related to PPC calls that started before the failure occurred.

2. The SCP sends an UNRELCALLDATA to the Serving MSC. The SCP's CNID parameter value is used to correlate the request to call data pertaining to recovery of the SCP failure.

3. The SSP compiles a list of stored call data that matches the received CNID value and for which no response was received to a TDISCONNECT or ODISCONNECT message. The SSP includes the time each of the calls ended. The SSP sends the requested information to the SCP in the CRREPORT.

4. Another failure occurs and the SCP does not respond to the SSP.

5. The SSP timer expires. The SSP executes local recovery procedures.

6. Conclusions

The WIN support is quite new area and this thesis is one of the earliest works in that field. The WIN standardization situation is not so clear at the moment, there are still some question without answers. And the time when WIN will be implemented in that selected network is not so clear at that moment. There are still a lot of things to do in that field, and this work could be a good start for the future activities. A lot of useful knowledge was collected during the work on this thesis, and those knowledge could be used in future if the decision of WIN support will be made.

7. References

[1]. IS-771 Wireless Intelligent Network, December 1998

[2]. PN-4289 Wireless Intelligent Network Capabilities
January 2000.

[3]. IS-826 Wireless Intelligent Network Capabilities For Pre-Paid Charging,
May 2000

[4]. "Mobile Telecommunications Networking with IS-41",
Gallagher,M., Snyder, R., McGraw-Hill, 1997

[5]. "The Global System for Mobile Communications",
Molly, M., Pautet, M.-B., 1992

[6]. www.3GPP.org