TTC標準
Standard

JT-Q1751

網間接続信号要求条件
IMT-2000 能力セット 1

Internetwork signalling requirements
for IMT-2000 capability set 1

第 1 版

2002 年 5 月 30 日制定

社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

Telecommunication Technology Committee

COPYRIGHTED MATERIAL

1) **本標準は、著作権者である** International Telecommunication Union **の文書による許諾を受け、**ITU **出版物を複製したものである。**

The ITU material has been reproduced with the prior authorization of the Union as copyright holder;

2) **複製に関わる責任は被許諾者にあり、**ITU **に帰するものではない。**

The sole responsibility for selecting extracts for reproduction lies with the beneficiary of this authrization alone and can in no way be attributed to the ITU;

3) ITU **出版物の入手先は下記による。**

The complete volume(s) of the ITU material, from which the texts reproduced are extracted, can be obtained from:

International Telecommunication Union
Sales and Marketing Service
Place des Nations – CH-1211 GENEVA 20 (Switzerland)
Telephone: +41 22 730 61 41 (English) / +41 22 730 61 42 (French) / +41 22 730 61 43 (Spanish)
Telex: 421 000 uit ch / Fax: +41 22 730 51 94
X.400:S=sales; P=itu; A=400net; C=ch
E-mail: sales@itu.int / http://www.itu.int/publications

網間接続信号要求条件 IMT-2000 能力セット 1

[Internetwork signalling requirements for IMT-2000 capability set 1]

＜参考＞ [Remarks]

１．英文記述の適用レベル [Application level of English description]

適用レベル [Application level]：E2

本標準の本文、付属資料および付録の文章および図に英文記述を含んでいる。

[English description is included in the text and figures of main body, annexes and appendices.]

２．国際勧告等の関連 [Relationship with international recommendations and standards]

本標準は、2000 年 6 月に ITU-T SG11 で承認された Recommendation Q.1751 に準拠している。

[This standard is standardized based on the Recommendation Q.1751 approved by ITU-T SG11 in June 2000.]

３．上記国際勧告等に対する追加項目等 [Departures from international recommendations]

3.1 **オプション選択項目** [Selection of optional items]

なし [None]

3.2 **ナショナルマター項目** [Items of national matter]

なし [None]

3.3 **原標準に対する変更項目** [Changes to original standard]

(1) 原標準が参照する標準のうち､TTC 標準に置き換える項目｡[Standards referred to in the original standard, which are replaced by TTC standards]

表１に示す。[Refer to Table 1.]

(2) 本標準で追加した項目。[Items added to the original standard]

なし [None]

(3) 本標準で削除した項目。ただし、本標準の理解を助けるために記述は残している。[Items deleted from the original standard]

なし [None]

(4) 本標準で修正した項目。[Items changed from the original standard]

なし [None]

3.4 **原標準との章立て構成比較** [Difference in chapter ordering from the original standard]

原標準との章立て構成の相違はない。

[There is no difference in chapter ordering from the original standard.]

４．改版の履歴 [Change history]

版数 [Revision]	制定日 [Date]	改版内容 [Contents]
第 1 版 [V.1]	2002 年 5 月 30 日	制定 [Newly standardized]

５．工業所有権 [IPR]

本標準に関わる「工業所有権等の実施の権利に係る確認書」の提出状況は、ＴＴＣホームページでご覧になれます。

６．その他 [Others]

なし [None]

表１　本標準で置き換えて参照する標準 [Table 1　Replaced standards referred]

原標準 [original standard]	置き換える標準 [replacement]
ITU-T 勧告 Q.1701 Title : Framework for IMT-2000 Networks	TTC 標準 JT-Q1701 Title : IMT-2000 網のフレームワーク
ITU-T 勧告 Q.1711 Title : Network Functional Model for IMT-2000	TTC 標準 JT-Q1711 Title : IMT-2000 網機能モデル
ITU-T 勧告 Q.1901 Title : Bearer independent call control protocol	TTC 標準 JT-Q1901 Title : ベアラに依存しない呼制御プロトコル

INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.1751

(06/2000)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for IMT-2000

Internetwork signalling requirements for IMT-2000 capability set 1

ITU-T Recommendation Q.1751

(Formerly CCITT Recommendation)

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4 AND No. 5	Q.120–Q.249
SPECIFICATIONS OF SIGNALLING SYSTEM No. 6	Q.250–Q.309
SPECIFICATIONS OF SIGNALLING SYSTEM R1	Q.310–Q.399
SPECIFICATIONS OF SIGNALLING SYSTEM R2	Q.400–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	**Q.1700–Q.1799**
BROADBAND ISDN	Q.2000–Q.2999

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation Q.1751

Internetwork signalling requirements for IMT-2000 capability set 1

Summary

This ITU-T Recommendation contains signalling requirements for the Network-to-Network Interface (NNI) protocol. The requirements are to support the capabilities that are recommended in the IMT-2000 Framework document and specified as Capability Set 1 (CS-1). This ITU-T Recommendation covers requirements for four communication groups of the NNI: Call and Bearer Control; Mobility Management; Virtual Home Environment (VHE) Service Control; and Packet Data Services and Internet Access Control. The requirements for inter-network security are described at a high level, and its functionality is incorporated into applicable communications group protocols. The requirements specified in this ITU-T Recommendation are non-information flow related, and they should be viewed as complementary to the information flows of ITU-T Recommendation Q.1721. They include general NNI protocol requirements, NNI functional models, NNI reference points, state models for selective functional entities, and the choice of various protocol suites.

Source

ITU-T Recommendation Q.1751 was prepared by ITU-T Study Group 11 (1997-2000) and approved under the WTSC Resolution 1 procedure on 15 June 2000.

Keywords

AMF, BICC, CN, CS-1, IMT-2000, INAP, LMFh, LMFv, MT, NNI, RAN, UIM, VHE.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSC Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

© ITU 2001

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the ITU.

CONTENTS

		Page
1	Scope	1
2	References	1
3	Definitions	2
4	Abbreviations	2
5	Introduction	5
6	General requirements	5
6.1	NNI requirements	5
6.2	VHE Service control requirements	6
6.2.1	Remote programming-based VHE	6
6.2.2	Service capabilities	6
6.3	CN data storage requirements for subscriber (user) profile	6
6.4	Global roaming requirement	7
6.5	NNI communication grouping	7
6.6	Internet services	8
6.7	Security Requirements	9
6.7.1	Requirements for the support of user authentication	9
6.7.2	Encryption requirements for Network-to-Network Interface	9
6.7.3	Key Management requirements for Network-to-Network Interface	9
7	Interconnection model	10
8	NNI functional interface	10
8.1	Functional model	10
8.2	Reference Points	11
8.2.1	Reference Point N01	12
8.2.2	Reference Point N02	12
8.2.3	Reference Point N03	12
8.2.4	Reference Point N04	12
8.2.5	Reference Point N05	12
8.2.6	Reference Point N06	13
8.2.7	Reference Point N07	13
8.2.8	Reference Point N08	13
8.2.9	Reference Point N09	13
8.2.10	Reference Point N10	13
8.2.11	Reference Point N11	13
8.2.12	Reference Point N12	13
8.2.13	Reference Point N13	14

Page

8.2.14 Reference Point N14 14
8.2.15 Reference Point N15 14
8.2.16 Reference Point N16 14
8.2.17 Reference Point N17 14
8.2.18 Reference Point N18 14
8.2.19 Reference Point N19 15
8.2.20 Reference Point N20 15
8.2.21 Reference Point N21 15

9 Protocol requirements for Mobility Management 15
9.1 Service drivers 15
9.2 Service logic interaction modes 16
9.3 LMFv State Model 16
9.3.1 State: v_Null 17
9.3.2 State: v_Initial Registration 18
9.3.3 State: V_Authentication Processing 18
9.3.4 State: V_Registration_pending 19
9.3.5 State: V_Active_registered 19
9.3.6 State: v_Inactive_registered 20
9.3.7 State: v_Denied 20
9.4 LMFh State Model 20
9.4.1 State H_Location_Unknown 21
9.4.2 State H_Registering 22
9.4.3 State H_Registered 22
9.4.4 State H_Old_Location_Cancelling_and_Registered 23
9.4.5 State_H_Exception 23
9.5 AMF state model 23
9.5.1 State: A_Null 24
9.5.2 State: Authentication_Processing 25
9.5.3 State: Awaiting_Challenge_Response 25
9.6 Mobility Management Functional Communications 25
9.7 Choice of Protocol Suite 26

10 Protocol requirements for VHE Service Control 26
10.1 General requirements 26
10.2 Service Control Functional Communications 27
10.3 Choice of Protocol Suite 28

11 Protocol requirements for Call and Bearer Control 28
11.1 General requirements 28
11.2 Choice of switching principles 28

Page

11.3 Call and Bearer Control functional communications 28
11.4 Choice of Protocol Suite 30
11.5 Multimedia calls 31
11.6 Multi-party calls 31
12 Protocol requirements for Packet Service Control 32
12.1 The PSCF to PSGCF Interface protocol 32
12.1.1 User plane requirements 33
12.1.2 Control plane requirements 33
12.2 The LMFp to LMFp Interface Protocol 33
Appendix I – Guidance on trigger concepts and usage 35
I.1 Purpose 35
I.2 Introduction 35
I.3 Principles and concepts 35
I.4 Dynamic trigger arming 36
I.5 Distribution of triggers 36

ITU-T Recommendation Q.1751

Internetwork signalling requirements for IMT-2000 capability set 1

1 Scope

The scope of this ITU-T Recommendation includes preparation of inter-networking signalling requirements to be used for development of a unique and common Network-to-Network Interface (NNI) protocol. With inputs from ITU-T Recommendations Q.1701 [1], Q.1711 [2] and Q.1721 [3], this ITU-T Recommendation provides signalling and protocol requirements, that are not of information flow nature. Specifically, this ITU-T Recommendation includes the following subjects:

- Description of the signalling layers in accordance with the functional groupings for Call and Bearer Control (CBC), Mobility Management (MM), Packet Services Control (PSC), and VHE Service Control (VSC).
- NNI instances for Global Roaming and their Reference Points.
- State Models for various Functional Entities.
- Signalling Requirements for NNI Protocol(s).
- Choice of NNI Protocols.

The CN-CN interworking can also be realized by specifying an interworking function (IWF) for protocol (and billing) information conversion between different family members. But the detailed specification of the interworking function is outside the scope of ITU.

Preparation of detailed description using "Specification and Description Language" (SDL), design of the protocol architecture and coding of the protocol are beyond the scope of this ITU-T Recommendation.

Aspects of OAM between Family Member Systems are also beyond the scope of this ITU-T Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[1] ITU-T Recommendation Q.1701 (1999), *Framework for IMT-2000 networks.*

[2] ITU-T Recommendation Q.1711 (1999), *Network functional model for IMT-2000.*

[3] ITU-T Recommendation Q.1721 (2000), *Information flows for IMT-2000 capability set 1.*

[4] ITU-T Recommendation Q.1901 (2000), *Bearer independent call control protocol.*

[5] ITU-T Recommendation Q.2630.1 (1999), *AAL type 2 signalling protocol (Capability Set 1).*

[6] ITU-T Recommendations Q.1238 series, *Interface Recommendation for intelligent network capability set 3.*

[7] ITU-T Recommendation Q.1290 (1998), *Glossary of terms used in the definition of intelligent networks.*

3 Definitions

This ITU-T Recommendation defines the following terms:

3.1 anchor core network: In a data session roaming environment, the anchor core network is the network where the data session is initiated and a packet service gateway is assigned to the mobile terminal. The anchor core network may be either the home or the visited network.

3.2 reference point: In an inter- or intra-network functional model, the point of reference is referred to the relationship between two functional entities for exchanging signalling messages and operations transactions.

3.3 service application: The provision of services by general purpose capabilities, such as Intelligent Network capabilities as applied at the home location or at a visited location as part of a Virtual Home Environment.

3.4 service control: Functions that set or modify the context in which basic calls and bearers are established, modified and released.

3.5 state model: The state model for a functional entity is a schematic representation of the states of a functional entity in relation to an inter-network signalling procedure. It includes identification of all entry and exit Detection Points (DPs) for each state.

3.6 subscriber: The user of a mobile terminal who has subscribed to the service.

3.7 supplementary service application: The provision of a specific supplementary service, typically through use of service specific capabilities, whether at the home location or at the visited location as part of a Virtual Home Environment.

3.8 user: The user of a mobile terminal. The terms "user" and "subscriber" are used interchangeably in this ITU-T Recommendation.

3.9 virtual home environment: The provision of a service experience to the visiting subscriber identical to, or as similar as possible to the service experience the subscriber has when served at his home location.

This ITU-T Recommendation uses terms defined in ITU-T Recommendation Q.1701 [1].

– **core network**

This ITU-T Recommendation uses terms defined in ITU-T Recommendation Q.1290 [7].

– **functional entity**

– **detection point**

– **service trigger**

4 Abbreviations

This ITU-T Recommendation uses the following abbreviations:

AALx	ATM Application Layer x
AC	Authentication Centre
ADDS	Application Data Delivery Service
AINI	ATM InterNetwork Interface
AMF	Authentication Management Function
ATM	Asynchronous Transfer Mode
BICC	Bearer Independent Call Control

B-ISUP	Broadband ISUP
CBC	Call and Bearer Control
CC	Call Control
CCAF'	Call Control Agent Function (enhanced, as described in ITU-T Recommendation Q.1711 [2])
CCF	Call Control Function
CCF'	Call Control Function (enhanced, as described in ITU-T Recommendation Q.1711 [2])
CLI	Calling Line ID
CN	Core Network
CNa	Core Network (anchored)
CnCAF	Connection Control Agent Function
CnCF	Connection Control Function
CNh	Core Network (home)
CNpv	Core Network (previous visited)
CNsn	Core Network (supporting)
CNv	Core Network (visited)
CS-X	Capability Set X
DFP	Distributed Functional Plane
DP	Detection Point
FE	Functional Entity
FT	Fixed Terminal
GPCF	Geographic Position Control Function
GPF	Geographic Position Function
GTT	Global Title Translation
ID	Identity
IF	Information Flow
IMDN	IMT-2000 International Mobile Directory Number
IMT-2000	International Mobile Telecommunications-2000
IMUI	IMT-2000 International Mobile User Identity
IN	Intelligent Network
INAP	Intelligent Network Application Protocol
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISUP	ISDN User Part
IWF	InterWorking Function

LAI	Location Area Identity
LMF	Location Management Function
MCF	Mobile Control Function
MGPF	Mobile Geographic Position Function
MM	Mobility Management
MRTR	Mobile Radio Transmission and Reception
MSC	Mobile Switching Centre
MT	Mobile Terminal
NAI	Network Access Identifier
N-ISUP	Narrow-band ISUP
NNI	Network-to-Network Interface
Nxx	Reference Point Nxx
PDN	Packet data Network
PIAM	Point in Authentication Management
PIN	Personal Identification Number
PNNI	Private Network-to-Network Interface
PSC	Packet Service Control
PSCAF	Packet Service Control Agent Function
PSCF	Packet Service Control Function
PSGCF	Packet Service Gateway Control Function
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RACAF	Radio Access Control Agent Function
RAN	Radio Access Network
RF	Radio Frequency
RFTR	Radio Frequency Transmission and Reception
RNC	Radio Network Controller
SACF	Service Access Control Function
SCF	Service Control Function
SCP	Service Control Point
SDF	Service Data Function
SDP	Service Data Point
SIBF	System Access Information Broadcast Function
SLP	Service Logic Program
SMF	Service Management Function
SMS	Short Message Service
SRF	Specialized Resource Function

SSD	Shared Secret Data
TMUI	Temporary Mobile User Identifier
UDP	User Datagram Protocol
UIM	User Identity Module
UIMF	User Identification Management Function
UPT	Universal Personal Telecommunication
VHE	Virtual Home Environment
VSC	VHE Service Control

5 Introduction

The NNI signalling requirements identified in this ITU-T Recommendation are to assist protocol designers to develop specific protocols that govern the interactions among core networks of the IMT-2000 Family of Systems. These requirements are divided into two parts, applications and protocols, and organized into 12 clauses as follows. Clauses 1 through 5 are general documentation requirements providing description of the scope of this ITU-T Recommendation, a short summary of the content of this ITU-T Recommendation, references, abbreviations, definitions and terminology, and this introduction. Clause 6 contains all general and application related requirements including service capabilities, data storage and subscriber profile requirements. It also covers all functional modelling aspects of the NNI. Clause 7 identifies and describes all the protocol-related FE-to-FE reference points. A total of 20 reference points are addressed in this clause. Clauses 8 through 12 are related to the protocol requirements for five categories of signalling for call and bearer control, mobility management, VHE and IN service control, packet and internet service control, and inter-core network exchange of security information and data.

6 General requirements

6.1 NNI requirements

The NNI shall support the set of IMT-2000 CS-1 service/network capabilities and features that ensure backward compatibility with second generation systems.

The following set of numbered NNI requirements provides as a starting point to build a complete set in subsequent sections. The requirements are intentionally kept single objective oriented to enable easy and efficient traceability.

1) The NNI should provide for "look ahead" or optimum routing, e.g. to prevent the "tromboning" effect.[1]

2) The NNI should support the transfer of Call Detail Record (CDR) such as call reference tags, charging related data, advice of charge, and other CDR information needed for regulatory issues.

3) NNI should support messaging services (e.g. voicemail notification and ADDS).

---

[1] In second generation systems, tromboning causes a mobile terminated call to be routed back to the called mobile subscriber's home system, even if the called party may actually be in the calling party's vicinity. Especially in a global roaming situation, avoiding tromboning would be very beneficial, preventing long-distance trunk resource wastage.

6.2 VHE Service control requirements

Virtual Home Environment must be provided according to the scenarios identified in Q.1711 [2]. Two scenarios are identified in this ITU-T Recommendation:

Direct home command: This scenario calls for invocation of service logic to query for instruction/information to the SCFsn. In this scenario, the prearrangement between the supporting and the home networks or between the supporting and the visited networks may need screening capabilities of triggering invocation.

Relay service control: This scenario calls for the invocation of the service logic via the SCFh or the SCFv to query for instruction/information to the SCFsn. In this scenario the prearrangement between the supporting and the home networks or between the supporting and the visited networks ranges from relaying, security/screening capabilities to shared service logic.

6.2.1 Remote programming-based VHE

Support of VHE by means of downloading of service logic and service related data from the home network to both the serving network and the UIM.

6.2.2 Service capabilities

Charging: The Charging procedures are used to provide Call Documentation and Call Duration.

Network management: Network management procedures provide protection of the home network from overload.

Caller interaction and specialized resource handling: The procedures allow for playing announcements, prompting and collecting post-dialling information from the user (e.g. PIN for Credit Card Calling).

Assist and handoff: The procedures allow to request assistance to external equipment (e.g. IP) for playing announcement, prompting and collecting information.

6.3 CN data storage requirements for subscriber (user) profile

The following information items are stored in the subscriber home network and the subject of the subscriber information and profile management activities:

- IMT-2000 Mobile Directory Number (IMDN), e.g. a diallable number;
- IMT-2000 Mobile User ID (IMUI);
- IMT-2000 Temporary Mobile User ID (TMUI);
- Terminal State;
- User/Terminal Location Information;
- Basic Service Data (e.g. subscribed bearer services);
- Teleservices (e.g. broadcast and/or group call subscription data);
- Supplementary Services data;
- Operator Determined features/services (e.g. Call Barring Data);
- Subscriber Determined features/services (e.g. Call Screening Data);
- Roaming Restriction Data;
- Regional Subscription Data; and
- VHE Subscription Data.

6.4 Global roaming requirement

The NNI is a common and unique CN-to-CN interface protocol that supports the global roaming capability of the IMT-2000 and provides home service environment to the users roaming through two or more IMT-2000 family member networks. Figure 6-1 shows the role that the common NNI can play, in conjunction with various family members' IWFs, to provide interoperability among the networks and support global roaming by providing a home service environment to the roaming users. The implementation of the interoperability and the global roaming configuration as shown in Figure 6-1 has the following distinct characteristics over the implementation of IWFs for every core network pair.

- Open interface: There will be only one common and unique NNI (under development by ITU-T).
- Efficiency: One IWF (as opposed to N-1 bilateral IWFs) per family member for an IMT-2000 family of N members is needed. This is for every family member to interwork with all other family members.
- Transparency: Changes in one family member's network specifications will not affect other family members' IWFs.
- Future Proof: Can easily accommodate new members into the family.

While the development of the NNI protocol lies with ITU-T, the development of the IWF is the responsibility of each family member.

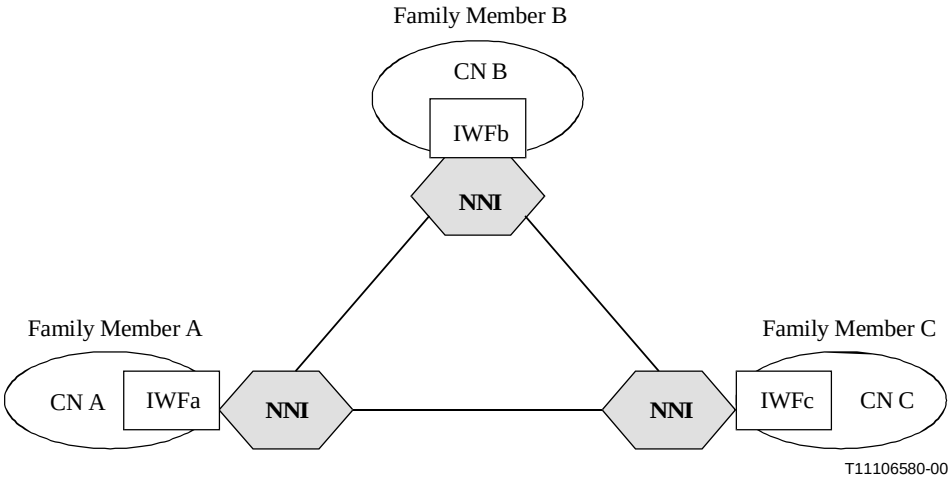


Figure 6-1/Q.1751 - IMT-2000 network interconnection model

6.5 NNI communication grouping

Four main and distinct communication groups are recognized in an IMT-2000 cross-CN operation. The distinction stems from the nature of the operations they support by constituting a unique and common NNI Application Protocol. These communications groups are as follows:

- *Call and Bearer Control (CBC)*

  This communication group includes all cross-CN exchange of information related to controlling connection-oriented and connectionless services including basic services, standard supplementary services.

- *Mobility Management (MM)*

  This communication group includes all cross-CN exchange of information related to mobility management (e.g. registration, authentication, and location information management).

- *VHE Service Control (VSC)*

  This communication group includes all cross-CN exchange of information related to the control of the home network services accessible from the visited networks.

- *Packet Service Control (PSC)*

  This communication group includes all cross-CN exchange of information related to the control of Packet services (e.g. voice, image and data).

The requirements for inter-network security are described at a high level, and its functionality is incorporated into applicable communications group protocols.

Within the context of a unique and common NNI protocol described in 6.4, this grouping is further illustrated in Figure 6-2 below:

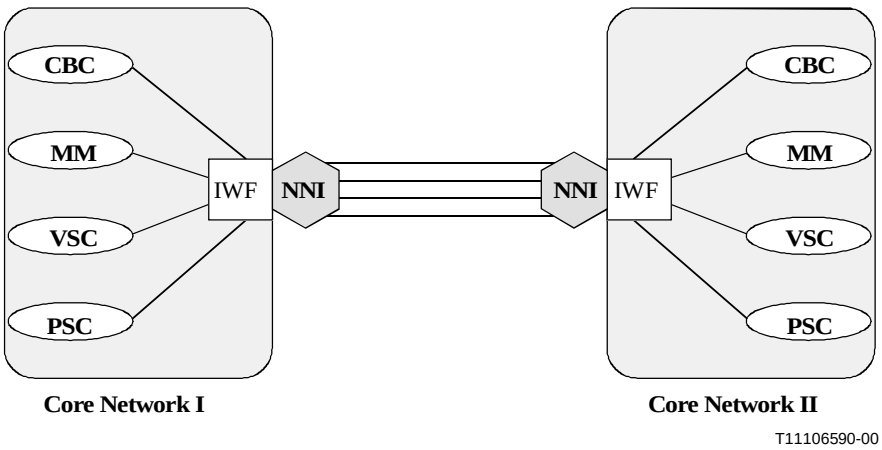


Figure 6-2/Q.1751 - NNI communications grouping

To set up a call and/or to transport a service across a protocol interfacing two core networks, one or more of these communications groups are to be established either directly or indirectly between two or more core networks. The interconnections scheme to carry out the required communications follows the IMT-2000 network interconnectivity model of clause 7, as illustrated in Figure 7-1.

6.6 Internet services

1) The roaming packet data subscriber should be able to gain access to public Internet, to a home ISP, or to a private network from multiple IMT-2000 service providers while maintaining a formal customer-vendor relationship with only one IMT-2000 service provider.

2) The subscriber should explicitly indicate which access data service (i.e. access to public Internet, to a home ISP, or to a private network) is being requested.

3) The subscriber should be able to establish simultaneous data sessions to public Internet, a home ISP, or a private network and have different IP addresses and NAIs for the respective access services. The packet data network may use the destination IP address or the NAI that may be included in the session registration request to determine the destination of the packet data session.

4) The NNI should be able to support QoS by assigning the user's traffic to a specific differentiated service class on a per packet basis for transport over the Internet. The NNI should be also able to assign all user's traffic to a specific service class on a per destination basis.

6.7 Security Requirements

The NNI is the interface point of an IMT-2000 system's core network to other core networks. The NNI interacts with other networks to provide end-to-end communication between users (see Figure 6-1). The NNI will transport information about users (e.g. location, authorization, authentication and encryption keys) and networks (i.e. signalling and control); this information must be kept secured from intruders. This ITU-T Recommendation addresses the security aspects of the information transport.

Security requirements for NNI can be separated into three parts. Authentication requirements (which includes privacy), Encryption requirements, and Key Management requirements for NNI. These parts are detailed below.

6.7.1 Requirements for the support of user authentication

- The NNI standards should be designed to allow for the possible introduction of new authentication algorithms, key sizes and optional authentication methods during the expected lifetime of the standards.
- The NNI security mechanisms should minimize the impact to the network traffic (e.g. by optionally allowing sharing of secret data between the home entity and the serving entity).
- The NNI security mechanisms should support unique challenges of terminals on dedicated (bearer and signalling) channels.
- The NNI security mechanism should support a global challenge mechanism, broadcast on a global signalling channel, requiring a terminal to correctly respond to a network challenge before dedicated channels are allocated.
- The NNI security mechanisms should be able to detect and report security violations, and have recovery mechanisms to restore the system to a protected state.
- The provision or the generation of privacy and encryption keys may be part of the authentication procedure.
- The compromise of an individual mobile shall not compromise the overall network security.

6.7.2 Encryption requirements for Network-to-Network Interface

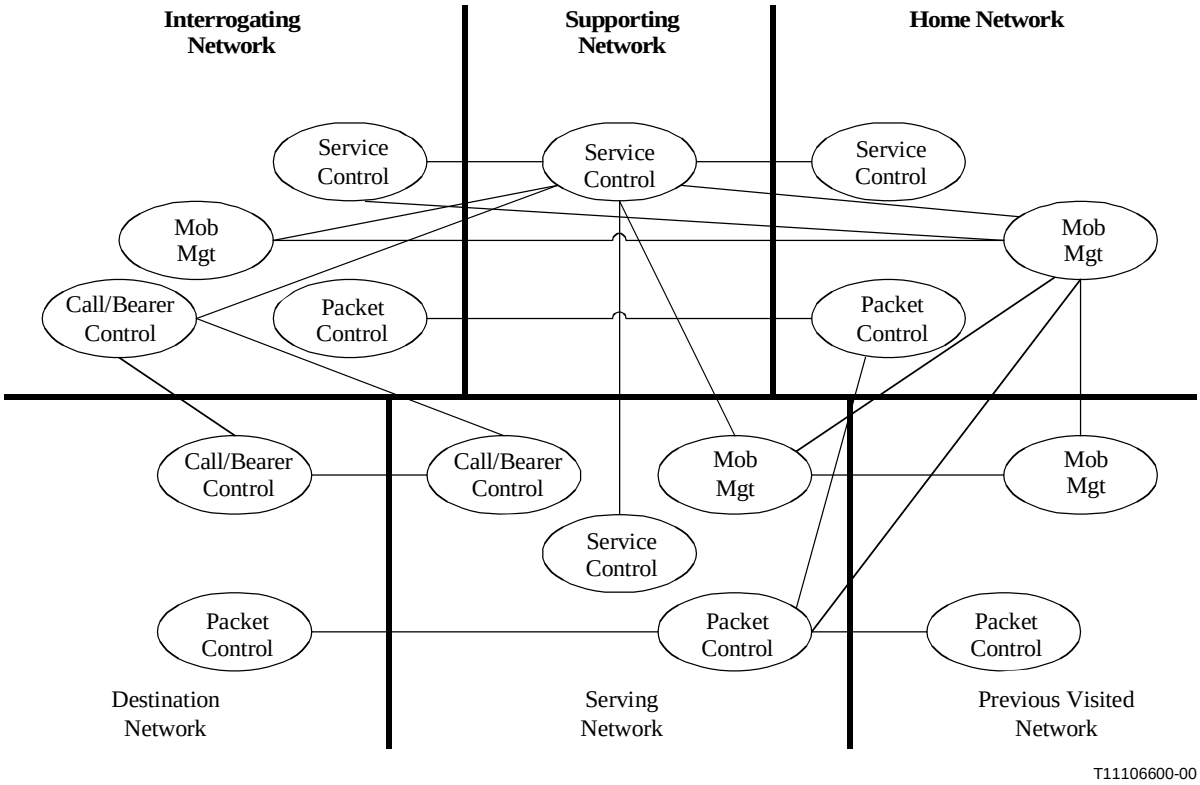
- The NNI encryption mechanisms should satisfy legal requirements imposed by regulation agencies (for example, export controls, lawful interception).
- The NNI encryption mechanisms should be able to encrypt in multi-megabits per second, without any compromise to security.
- The NNI security should be able to provide for mutual authentication among the network elements.

6.7.3 Key Management requirements for Network-to-Network Interface

- Compromise of a privacy key should not compromise authentication.
- Keys for data privacy may be based on the same authentication root key.
- The NNI encryption mechanisms should support call related key management, e.g. creation, distribution, modification, or revocation of cryptographic keys.
- The NNI shall not support modifications to the Authentication Root Key(s) stored in a UIM and the home authentication centre (AMFh).

7 Interconnection model

Figure 7-1 illustrates the relationships required to be supported by the NNI in support of IMT-2000 CS-1. All the FEs contained within each network are not necessarily shown here (e.g. Home network may contain SCF and SDF, Previously Visited network may contain PSGCF). Rather, the differentiation across NNI boundaries is intended to show which FEs are relevant to the particular network function for NNI interoperability. To avoid cluttering of the figure, no intra-network relationships are shown in the figure.



Service Control	SCF, SDF, SRF
Mobility Management	LMF, AMF, UIMF
Call and Bearer Control	CCF'/SSF, CnCF, SACF
Packet Control	PSCF, PSGCF

Figure 7-1/Q.1751 - IMT-2000 network interconnection model

8 NNI functional interface

8.1 Functional model

Figure 8-1 shows the "NNI Functional Interface Model". Its purpose is to focus this ITU-T Recommendation on only those interfaces that pertain to the NNI on a functional level. Figure 7-1 "IMT-2000 Network Interconnection Model" (NIM) and Figure 8-1 "NNI Functional Interface Model" (FIM) together provide the framework for identifying the NNI signalling relationships and the basis for defining the protocol.

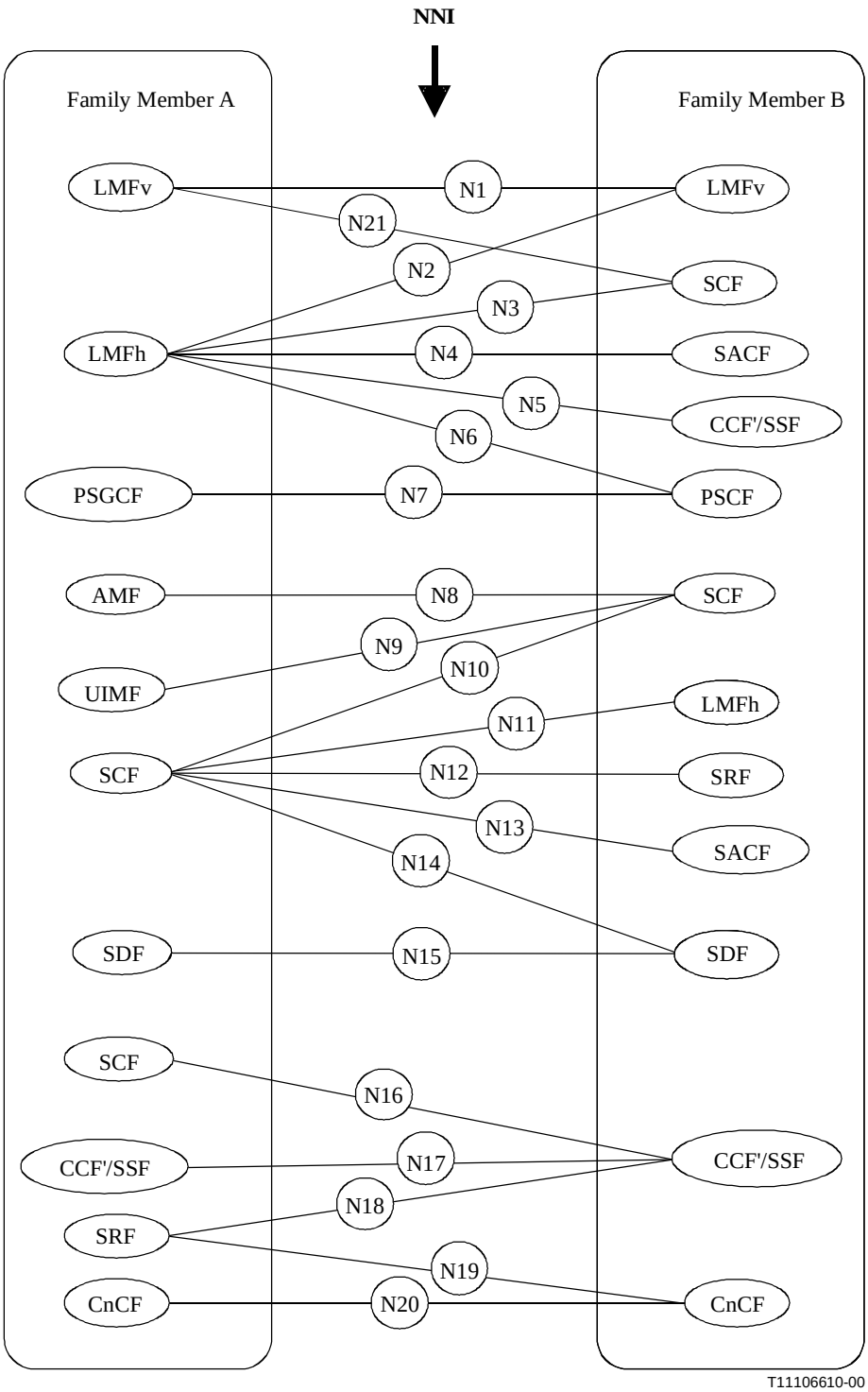


Figure 8-1/Q.1751 - NNI Functional Interface Model

8.2 Reference Points

The Reference Points (Nxx), shown in Figure 8-1, are described below with illustrative examples of the NNI messaging (extracted from clause 5 "The IMT-2000 Functional Models" in ITU-T Recommendation Q.1711[2]).

---

[2] Some of the relationships may not be covered in clause 7/Q.1711 [2]: "Global Roaming and Interworking Scenarios", perhaps because they were not meant to be comprehensive.

Note that to support IMT-2000 service requirements, the means of identifying subscribers needs to be extended to include IMUI and others. This is a general requirement, which is applicable to existing IN interfaces.

8.2.1 Reference Point N01

Reference Point N01 is the LMFv to LMFv functional interface. For example, NNI messaging over this functional interface enables:

- the management of subscriber information (e.g. for IMUI retrieval based on TMUI).

8.2.2 Reference Point N02

Reference Point N02 is the LMFh to LMFv functional interface. For example, NNI messaging over this functional interface enables:

- registration;
- registration cancellation (home to previously visited);
- the transfer of service profile;
- the transfer of routing information for the establishment of calls;
- the management of subscriber information;
- the control of supplementary services.

8.2.3 Reference Point N03

Reference Point N03 is the LMFh to SCF functional interface. For example, NNI messaging over this functional interface enables:

- location management related IN services.

8.2.4 Reference Point N04

Reference Point N04 is the LMFh to SACF functional interface. For example, NNI messaging over this functional interface enables:

- the transfer of routing information for the establishment of calls;
- the transfer of authentication related requests;
- the management of basic mobility information, such as:
  - MT location, status and identity;
- sharing of paging strategy information;
- the control of supplementary services;
- delivery of messages, such as:
  - SMS messages,
  - ADDS messages;
- managing global random challenge activities;
- managing unique authentication challenge activities.

8.2.5 Reference Point N05

Reference Point N05 is the LMFh to CCF'/SSF functional interface. For example, NNI messaging over this functional interface enables:

- the transfer of routing information for the establishment of calls;
- the transfer of profile information including service capability, such as:
  - protocol information;

– bearer information.

8.2.6 Reference Point N06

Reference Point N06 is the LMFh to PSCF functional interface. For example, NNI messaging over this functional interface enables:

- accessing and updating subscriber-related data;
- updating packet service information;
- updating packet routing information.

8.2.7 Reference Point N07

Reference Point N07 is the PSGCF to PSCF functional interface. For example, NNI messaging over this functional interface enables:

- the updating of MT packet data service information;
- the updating of MT routing context association;
- transfer of user data between an MT and a packet network.

8.2.8 Reference Point N08

Reference Point N08 is the AMF to SCF functional interface. For example, NNI messaging over this functional interface enables:

- user authentication related IN services.

8.2.9 Reference Point N09

Reference Point N09 is the UIMF to SCF functional interface. For example, NNI messaging over this functional interface enables:

- the transfer of service data/logic;
- the modification of service profile;
- the exchange of application information.

8.2.10 Reference Point N10

Reference Point N10 is the SCF to SCF functional interface. For example, NNI messaging over this functional interface enables:

- the acquisition and manipulation of secured data;
- distributed service control;
- unsolicited service notifications.

8.2.11 Reference Point N11

Reference Point N11 is the SCF to LMFh functional interface. For example, NNI messaging over this functional interface enables:

- the LMFh to provide MT location and subscriber status to the SCF.

8.2.12 Reference Point N12

Reference Point N12 is the SCF to SRF functional interface. For example, NNI messaging over this functional interface enables:

- the provision of specialized resources for IN services.

8.2.13 Reference Point N13

Reference Point N13 is the SCF to SACF functional interface. For example, NNI messaging over this functional interface enables:

- IN services based on mobility management events, such as:
  - location management;
  - user authentication;
- call unrelated IN services.

8.2.14 Reference Point N14

Reference Point N14 is the SCF to SDF functional interface. For example, NNI messaging over this functional interface enables:

- the SDF to provide the SCF with a logical view of subscriber data;
- the SCF and SDF to manage and update service data.

8.2.15 Reference Point N15

Reference Point N15 is the SDF to SDF functional interface. For example, NNI messaging over this functional interface enables:

- the exchange of service data.

8.2.16 Reference Point N16

Reference Point N16 is the SCF to CCF'/SSF functional interface. For example, NNI messaging over this functional interface enables:

- call related IN services.

8.2.17 Reference Point N17

Reference Point N17 is the CCF'/SSF to CCF'/SSF functional interface. For example, NNI messaging over this functional interface enables:

- the management of call instances with respect to:
  - establishment;
  - maintenance;
  - release;
- the management of CCF'-based services including CCF'-CCF' interactions (e.g. redirection request).

8.2.18 Reference Point N18

Reference Point N18 is the SRF to CCF'/SSF functional interface, when call and connection control are integrated. For example, NNI messaging over this functional interface enables:

- the control of bearers to SRF for IN services, with respect to:
  - establishment;
  - maintenance;
  - release.

Note that as an option, BICC (Bearer Independent Call Control) protocol could also be used across this reference point.

8.2.19 Reference Point N19

Reference Point N19 is the SRF to CnCF functional interface, when call and connection control are separated. For example, NNI messaging over this functional interface enables:

- the control of bearers to SRF for IN services, with respect to:
  - establishment;
  - maintenance;
  - release.

8.2.20 Reference Point N20

Reference Point N20 is the CnCF to CnCF functional interface. For example, NNI messaging over this functional interface enables:

- the management of connection instances, with respect to:
  - establishment;
  - maintenance;
  - modification;
  - release.
- the management of bearer control associations, with respect to:
  - establishment;
  - maintenance;
  - release.

8.2.21 Reference Point N21

Reference Point N21 is the LMFv to SCF functional interface. For example, NNI messaging over this functional interface enables:

- location management related IN services.

9 Protocol requirements for Mobility Management

9.1 Service drivers

The following IN service drivers are detailed further in this ITU-T Recommendation, and are used as example of IN services based on mobility events:

1) **Credit Check**: The subscriber may be refused registration when roaming if he has no more credit. In a similar way, he may be notified when his account has reached a predetermined threshold. Eventually, he may be authorized to register only for a restricted set of services if a certain threshold has been reached.

2) **Authentication Location Control**: The subscriber may be refused registration if a fraud has been detected. Consistency between successive registration location is checked: for instance, the subscriber has registered in Berlin, and 15 minutes later in Chicago. Authentication location check helps detecting such fraud.

3) **UPT**: IMT-2000 is required to support UPT. It is assumed here that a UPT user is allowed to register on a mobile terminal from that terminal: UPT registration is based on an IMT-2000 number, i.e. a mobile subscriber must be registered on the terminal before a UPT user starts registering. For efficient routing, the UPT SCF needs to be notified when the terminal is switched off or on in order to route the call to the appropriate destination (e.g. to the UPT voicemail when the terminal is off). In a similar manner, the UPT service may include

service restrictions when the mobile terminal is roaming: the UPT SCF must be notified when the terminal registers in a visited network in order to check roaming authorization for the UPT user and to apply specific charging for both incoming and outgoing calls.

4) **Local Advertising**: When the mobile subscriber registers, some advertising may be displayed in order to give him some local information, e.g. weather forecast. It depends on the service elements to which the user has subscribed.

5) **Dynamic Filtering based on User Location**: When in roaming, the subscriber may wish to filter incoming calls, if split charging is used. Dynamic filtering is activated when the user registers in a foreign visited network (roaming user) and as long as the terminal is on.

9.2 Service logic interaction modes

Among the service features detailed in 9.1, IN service logic controlling mobility management processing can be classified in two types as follows:

- **Notification**: The SCF is only notified by the LMF that a mobility event has occurred. UPT local advertising and filtering are considered of this type. The SCF does not influence the outcome of the mobility procedure, although the IN service is provided to the user. In the example, either a messaging service is provided, or another IN service, related or not to the subscriber, is notified.
- **Control**: The SCF is able to modify the outcome of the mobility procedure, for instance by denying or cancelling authentication or registration. The credit check and authentication location control are examples of such services.

9.3 LMFv State Model

Figure 9-1 is a schematic presentation of the LMFv state model showing various possible states of the mobile terminal in the visited network. It includes identification of all entry and exit Detection Points (DPs) for each state. These states and DPs are further described below.

DPs with no identified service drivers are shown in grey. In the future, these DPs may be removed if no service justification is provided. The removal of these DPs will not impact the validity of the model (including states, event, state transitions, and actions).

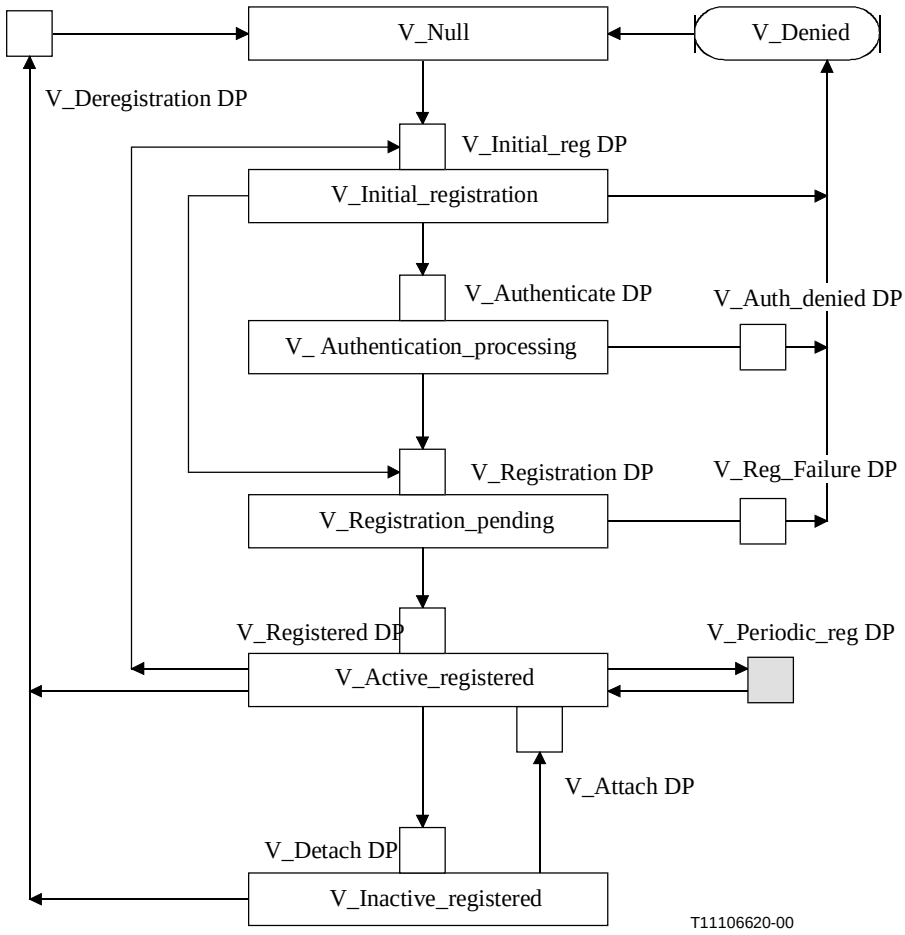


Figure 9-1/Q.1751 - LMFv state model

9.3.1 State: v_Null

Description

Initial state (the mobile user is not known in the LMFv) and LMFv awaits registration request.

Entry Events

- Receipt of location cancellation for the MT (DP: v_Deregistration).
- Handling of authorization or registration denied for the MT is completed (Transition from v_Denied).

Actions

- Removes the subscriber profile if present and releases any other resources allocated to the MT.

Exit Events

- A registration request is received for the MT (DP: v_Initial_reg).

9.3.2 State: v_Initial Registration

Description

The user registration is initiated and decision on authentication processing is made.

Entry Events[3]

- A registration request is received for the MT (DP: v_Initial_reg).
- A registration request is received for the MT for a new location area (while in the Active state) (DP: v_Initial_reg).

Actions

- Initiates the user registration, and gathers information on the user (e.g. authentication information and user identity from the previous visited network).
- Decides whether authentication is to be performed or not. The way this decision is made is operator specific.

Exit Events

- Authentication is to be performed: authenticate (DP: v_Authenticate).
- Authentication is not to be performed: do not authenticate (DP: v_Registration).
- Registration fails (Transition to v_Denied).

9.3.3 State: V_Authentication Processing

Description

Authentication is processed.

Entry Events[3]

- Authentication is needed (DP: v_Authenticate).

Actions

- Retrieves new authentication parameters if none available.
- Processes authentication.

Exit Events

- Authentication is successful (DP: v_Registration).
- Authentication failed (DP: v_Auth_denied).

[3] Considering real-time requirements in the network, these DPs should be implemented for notification without suspending location management processing (equivalent to TDP-N).

9.3.4 State: V_Registration_pending

Description

The registration for the MT is processed.

Entry Events[3]

- The MT has been successfully authenticated (DP: v_Registration).
- Authentication was not to be performed: do not authenticate (DP: v_Registration).

Actions

- Registration processing for the MT.
- A subscriber record is filled or updated with MT location information, authorization period and other information.
- The subscriber profile is retrieved.

Exit Events

- Registration succeeds (DP: v_Registered).
- Registration fails (DP: v_Reg_Failure).

9.3.5 State: V_Active_registered

Description

The MT is registered and it is assumed to be reachable.

Entry Events

- Registration has been successfully performed (DP: v_Registered).
- A registration request is received from a detached MT (DP: v_ Attach).
- A registration request is received for the MT in the same location area (DP: v_Periodic_reg).

Actions

- Maintains the MT location pointer and sets the MT status to active.
- If requested, provides a routing address for establishment of an information exchange path (e.g. call delivery, short message delivery). Requests paging before sending back a routing address [this is an option of the visited network].
- If requested, provides notification that the MT is successfully registered and active.
- If requested, provides information based on the subscriber's service profile.

Exit Events

- A registration request is received for the MT in the same location area (DP: v_Periodic_reg).
- A detach request is received for the MT (DP: v_Detach).
- A registration cancellation request is received for the MT (DP: v_Deregistration).
- A registration request is received for the MT in a new location area. (DP: v_Inital_reg).

9.3.6 State: v_Inactive_registered

Description

The MT is registered, but it is not reachable. The user data and service profile are still retained in the visited network.

Entry Events

- A detach request is received for the MT (DP: v_Detach).

Actions

- Maintains the MT location pointer and sets the MT status to inactive.
- If requested, informs that the MT is inactive.

Exit Events

- A registration request is received from the detached MT (DP: v_Attach).
- A registration cancellation request is received for the MT (DP: v_Deregistration).

9.3.7 State: v_Denied

Description

Handling of failure and denial from authentication and registration.

Entry Events

- Registration is denied during authentication (DP: v_Auth_denied) or location registration (DP: v_Reg_failure).

Actions

- Provides information about registration or authentication denial for the MT.
- Sets the Exception Timer.

Exit Events

- The Exception Timer elapses (Transition to v_Null).

9.4 LMFh State Model

This subclause provides a high-level description of the Location Management State Model for the LMFh (location management function), showing Points in Location Management (PILM) and Detection Points (DP). All of the possible DP-to-PILM and PILM-to-DP transitions are illustrated.

In the future, these DPs may be removed if no service justification is provided. The removal of these DPs will not impact the validity of the model (including states, event, state transitions, and actions).

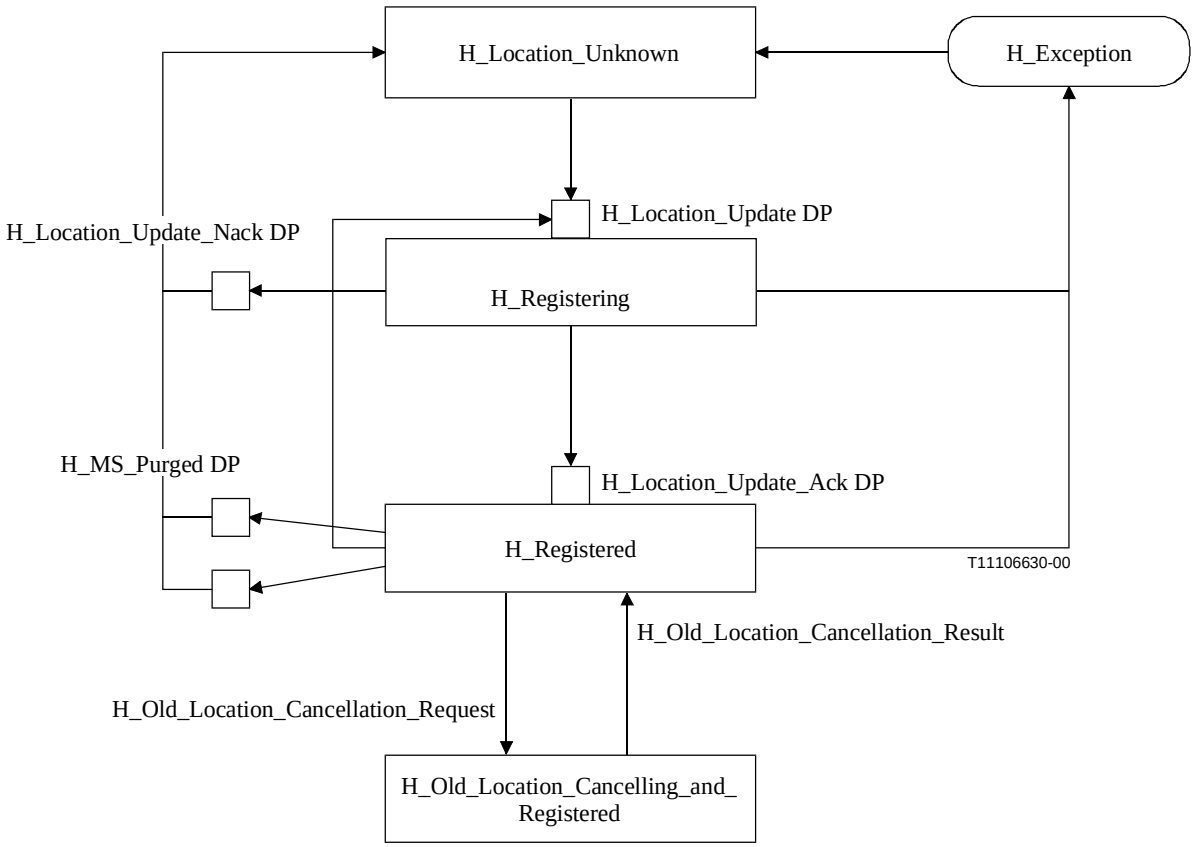


Figure 9-2/Q.1751 - LMFh Location Management State Model

9.4.1 State H_Location_Unknown

Description

The location of the Mobile Subscriber is unknown and terminating services (i.e. Mobile Call termination, SMS Termination, etc.) cannot be handled.

Entry Events

- Mobile Subscriber purged (DP: H_MS_Purged).
- Mobile Subscriber registration in visited domain cancelled by LMFh (DP: H_present_location_cancelled).
- An exception occurs (PILM: H_Exception).

Actions

None.

Exit Events

- Mobile Subscriber registered to the mobile network (DP: H_Location_Update, note restrictions as described in H_Registering state).

9.4.2 State H_Registering

Description

The Mobile Subscriber that changed between or attached to service area within the mobile network needs to transfer its service profile to the service area and the location information of the subscriber needs to be updated.

Entry Events[4]

- The Mobile Subscriber registered to the mobile network (DP: H_Location_Update).
- The Mobile Subscriber roamed between service areas (DP: H_Location_Update).

Actions

- Check if the subscriber is known within the database.
- Authorize the Mobile Subscriber network access.
- Transfer the Mobile Subscriber profile towards the new service area.
- Update the location information of the Mobile Subscriber within the database.

Exit Events

- Negative response to the location update request (i.e. such as subscriber unknown, subscriber rejected, etc.) (DP: H_Location_Update_Nack).
- Positive response to the location update request (DP: Location_Update_Ack).
- An exception occurs (PILM: H_Exception).

9.4.3 State H_Registered

Description

The location of the Mobile Subscriber is known and terminating services (i.e. Mobile Call termination, SMS Termination, etc.) can be handled.

Entry Events

- Successful location update (DP: H_Location_Update_Ack).
- Successful or unsuccessful location cancellation in old LMFv (PILM: H_old_registration_cancellation_result).

Actions

- Handle location requests for terminating services.
- Handle service profile updates in visited LMF. These profile updates will not impact ongoing call or other ongoing services.

Exit Events

- Decision to cancel registration (DP: H_present_location_cancelled).
- Decision to delete subscriber in old LMFv (PILM: H_old_location_cancellation_request).
- Indication from LMFv that the MS has been purged (DP: H_MS_Purged).
- The Mobile Subscriber roamed to another Service Area (DP: Location_Update, note restrictions as described in the H_Registering state).
- An exception occurs (PILM: Exception).

---

[4] Considering real-time requirements in the network, this DP should be implemented for notification without suspending location management processing (equivalent to TDP-N).

9.4.4 State H_Old_Location_Cancelling_and_Registered

Description

The subscriber record in the old LMFv is cancelled.

Entry Events

- Decision by LMFh to cancel location in old LMFv (PILM: H_Old_Location_Cancellation_Request).

Actions

- Interact with old LMFv to cancel location.
- Update management information of the Mobile Subscriber within the database.

Exit Events

- Successful or unsuccessful location cancellation (PILM: H_Old_Location_Cancellation_Result).

9.4.5 State_H_Exception

Description

Handling of failure and exceptions

Entry Events

- HLR exceptions occurring during the H_registered and H_registering states processing.

Actions

- Exception handling for a specific mobile subscriber.

Exit Events

- Exception handling completed (transition to H_Location_Unknown).

9.5 AMF state model

This provides a high-level description of the Authentication Management Function (AMF) State Model (see Figure 9-3) showing Points in Authentication Management (PIAM) and Detection Points (DP). All of the possible DP-to-PIAM and PIAM-to-DP transitions are illustrated. This AMF SM applies to both the home and the visited situations. An authentication state model instance is created in the AMF where authentication is processed. This excludes the process where authentication parameters are generated. Depending on the implementation, it is located either in the home or the visited network. The use of the home AMF or the visited AMF is an operator decision.

In the future, these DPs may be removed if no service justification is provided. The removal of these DPs will not impact the validity of the model (including states, event, state transitions, and actions).

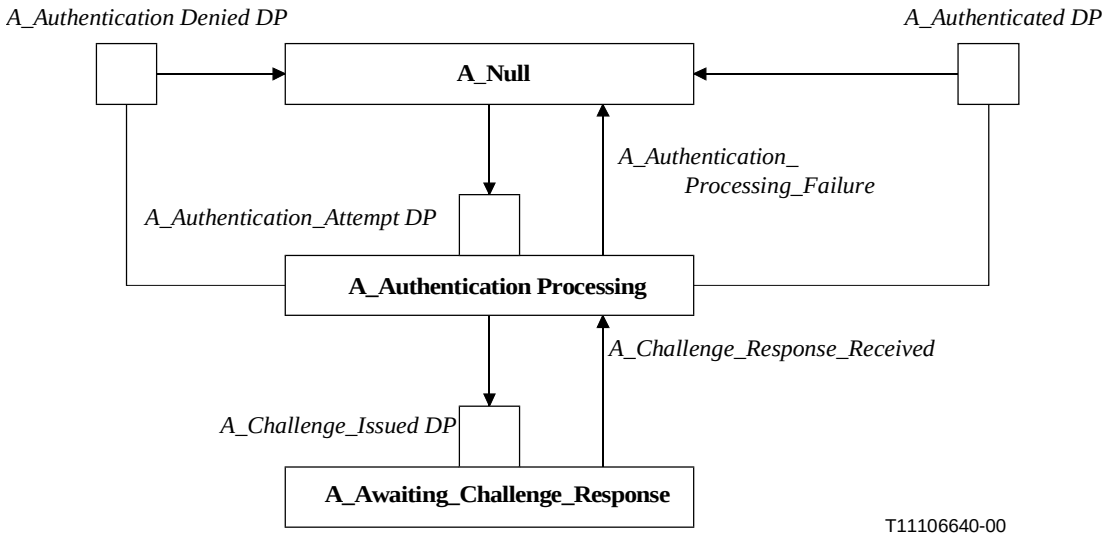


Figure 9-3/Q.1751 - AMF State Model

9.5.1 State: A_Null

Description

Initial state (the AMF awaits an authentication request from the mobile user).

Entry Events

- Authentication processing failure occurs (PIAM: A_Authentication_Processing_Failure).
- Authentication is denied (DP: A_Authentication_Denied DP).
- Authentication is successful (DP: A_Authenticated DP).

Actions

- None.

Exit Events

- An authentication request is received (DP: A_Authentication_Attempt).

9.5.2 State: Authentication_Processing

Description

The user authentication processing takes place.

Entry Events

- An authentication request is received (DP: A_Authentication_Attempt DP).
- The result of the Awaiting_Challenge_Response is received (PIAM: A_Challenge_Response_Received).

Actions

- Call count is updated if necessary.
- Privacy keys are generated if necessary.
- Authentication processing is performed and depending on the outcome of the State: A_Awaiting_Challenge_Response, either Authentication is successful or it is denied.

Exit Events

- Authentication processing failure occurs (PIAM: A_Null).
- An authentication challenge is issued (SCF processing could occur at this point) (DP: A_Challenge_Issued DP).
- Authentication is successful (DP: A_Authenticated).
- Authentication is denied (DP: A_Authentication_Denied).

9.5.3 State: Awaiting_Challenge_Response

Description

The AMF waits for a response to the authentication challenge.

Entry Events

- An authentication challenge was issued (DP: A_Challenge_Issued DP).

Actions

- None.

Exit Events

- The AMF receives a response to the authentication challenge (PIAM: A_Challenge_Response_Received).
- Authentication processing failure occurs (PIAM: A_Null).

9.6 Mobility Management Functional Communications

Figure 9-4 has been reproduced from ITU-T Recommendation Q.1711, extended to show the CN-CN interface.

The bold relationships fall – either fully or partially – within the scope of Mobility Management.

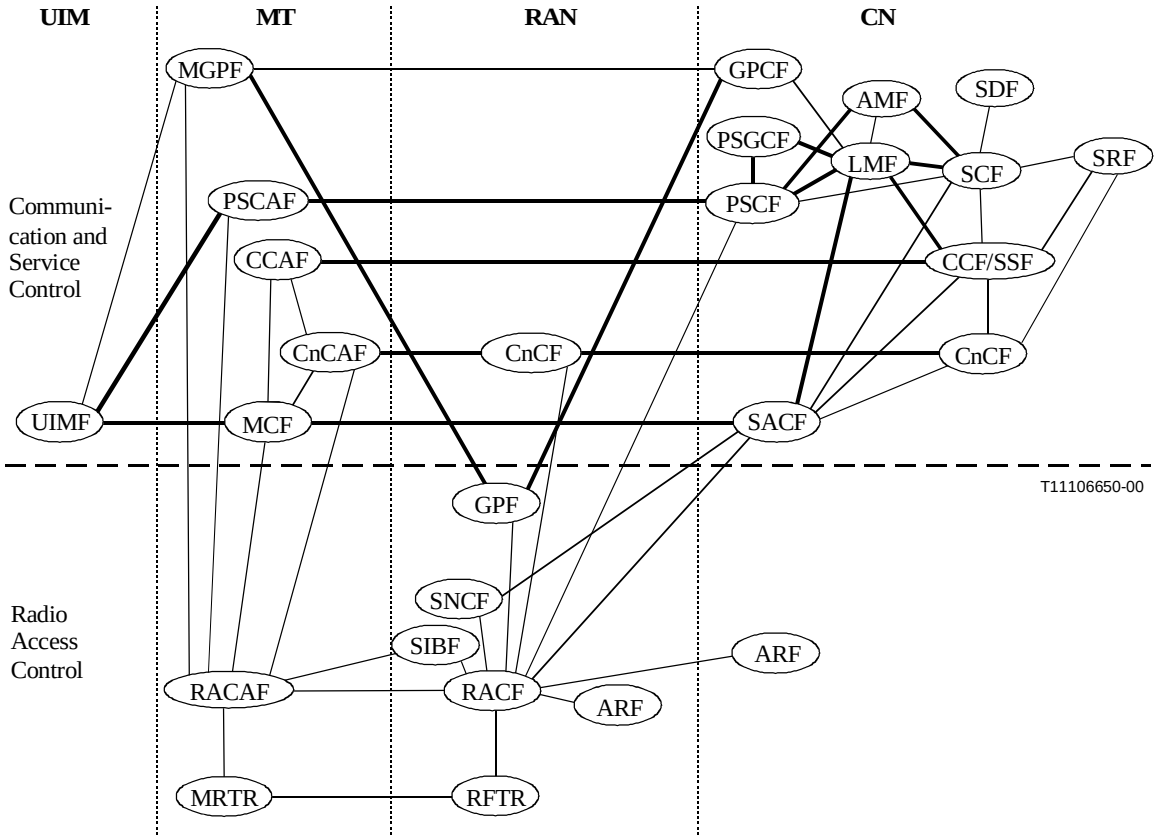


Figure 9-4/Q.1751 - The IMT-2000 Functional Model (Mobility Management)

9.7 Choice of Protocol Suite

Various mobility protocols already exist for 2G systems, such as GSM MAP and IS-41. They have all been specifically designed and optimized for these 2G systems and service capabilities. However, the main drawback of these protocols is that they cannot easily support inter-family communication because of their specific nature and design (i.e. the syntax and semantics of arguments and results of these Mobility Management operations are heavily coupled with the related 2G services and architecture).

The 2G protocols need enhancements to support the inter-family roaming between the different IMT-2000 members of systems. Therefore, the challenge of making the common NNI protocol for Mobility Management feasible for inter-family roaming relies mainly on creating protocol elements that should not be restricted to a particular mobile service and radio access technology. In other words, it should be generic enough to fit with the different members/systems of IMT-2000 from the NNI perspective. One way to proceed forward in that direction is to derive generic operations based on common parameters for IMT-2000 services that will be used by these different members. Attention should also be given to make the evolution path from the existing 2G systems towards the 3G common NNI as smooth as possible.

10 Protocol requirements for VHE Service Control

10.1 General requirements

1) For the VHE Service Invocation information elements addition of the following to the relevant operation definitions in INAP are recommended:

   - subscriber is a mobile subscriber;

- mobile subscriber identity (e.g. IMUI);
- terminal capabilities (e.g. voice, data, etc.);
- location information (e.g. latitude and longitude, cell site, elevation, precision, etc.).

2) The trigger profile that is dynamically and geographically placed needs to include, in addition to the identification of the triggers, trigger criteria and service logic addresses associated with the triggers, protocol version information to be used to the indicated service logic program. The protocol version is required to ensure that the message sent to the SLP is of a version not higher than the SLP that is equipped to recognize and deal with.

3) For the VHE service Information flows involving the use of a specialized resource, the information flows should be aligned with the IN specifications.

4) For the VHE service provisioning, the SCF and SRF in the "supporting network" might be anywhere. As such, appropriate addressing mechanisms are required. The addressing capabilities of the INAP protocol for this aspect should be reviewed to ensure adequacy.

10.2 Service Control Functional Communications

Figure 10-1 has been reproduced from ITU-T Recommendation Q.1711. It is extended here to show the CN-CN interface for the service control capability.

The bold relationships fall – either fully or partially – within the scope of Service Control Signalling.

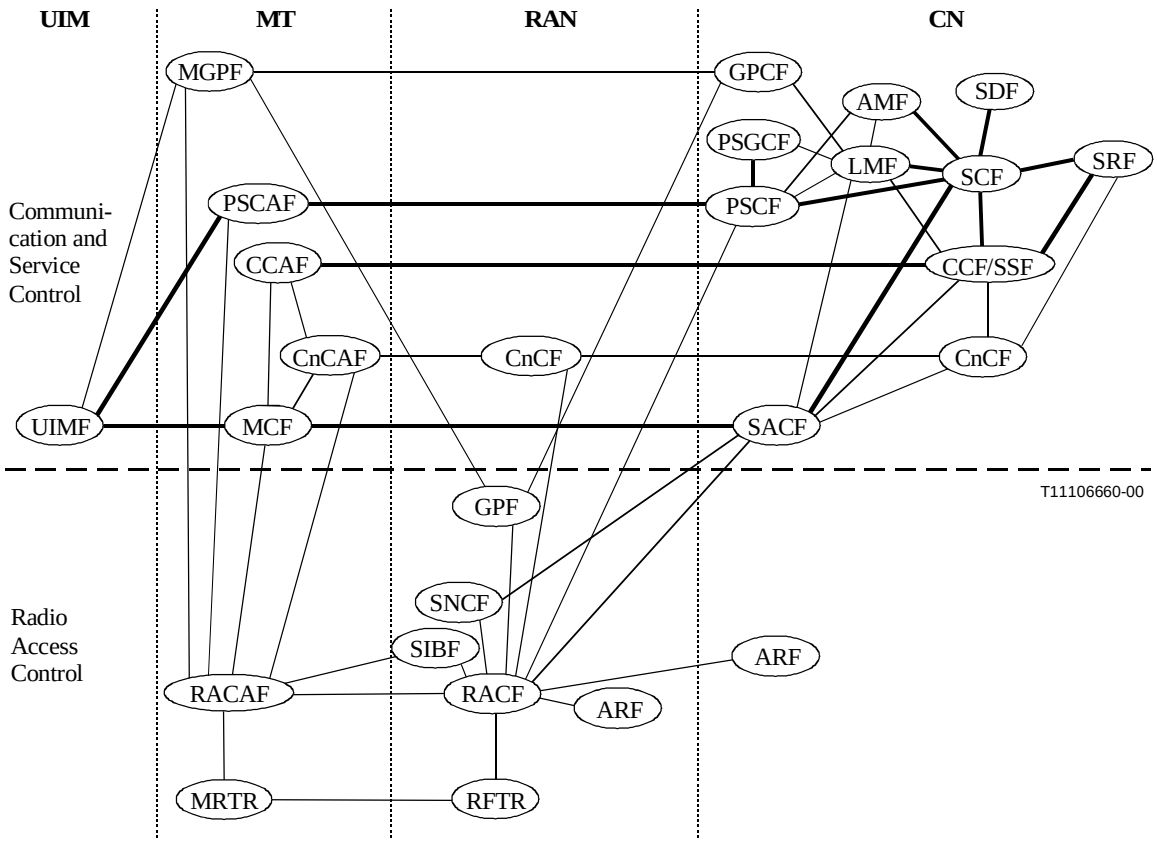


Figure 10-1/Q.1751 - The IMT-2000 Functional Model (Service Control)

10.3 Choice of Protocol Suite

Relationship	Initial Protocol Proposal
SCF-SDF	INAP + extensions for mobility.
SCF-SRF	INAP + extensions for mobility.
SCF-CCF'/SSF	INAP + extensions for mobility.
SCF-AMF	INAP-like based on AMF state model. Refer to clause 9/Q.1721 for information flows.
SCF-LMF	INAP-like based on LMF state model to be defined.
SRF-CCF'/SSF	Appropriate Bearer Control protocol.
SCF-UIMF (packet via PSCF, PSCAF)	Transport will be provided via IPv4 with potential evolution to IPv6.
SCF-UIMF (circuit, via SACF, MCF)	Options identified: • The ISDN USSD supplementary service will be used to support exchange of service/user dialogue. Refer to clause 11/Q.1721 for information flows. • IN CS-2 OCCRUI capability which makes use of ISUP APM and DSS1 GAT transport mechanism.

11 Protocol requirements for Call and Bearer Control

11.1 General requirements

Call Detail Record (CDR): This procedure allows to transfer CDR data from the serving network to the home network. Furthermore, real-time CDR transfer should be provided. However, in order to minimize data transfer only call reference tags and data necessary for call processing should be transferred.

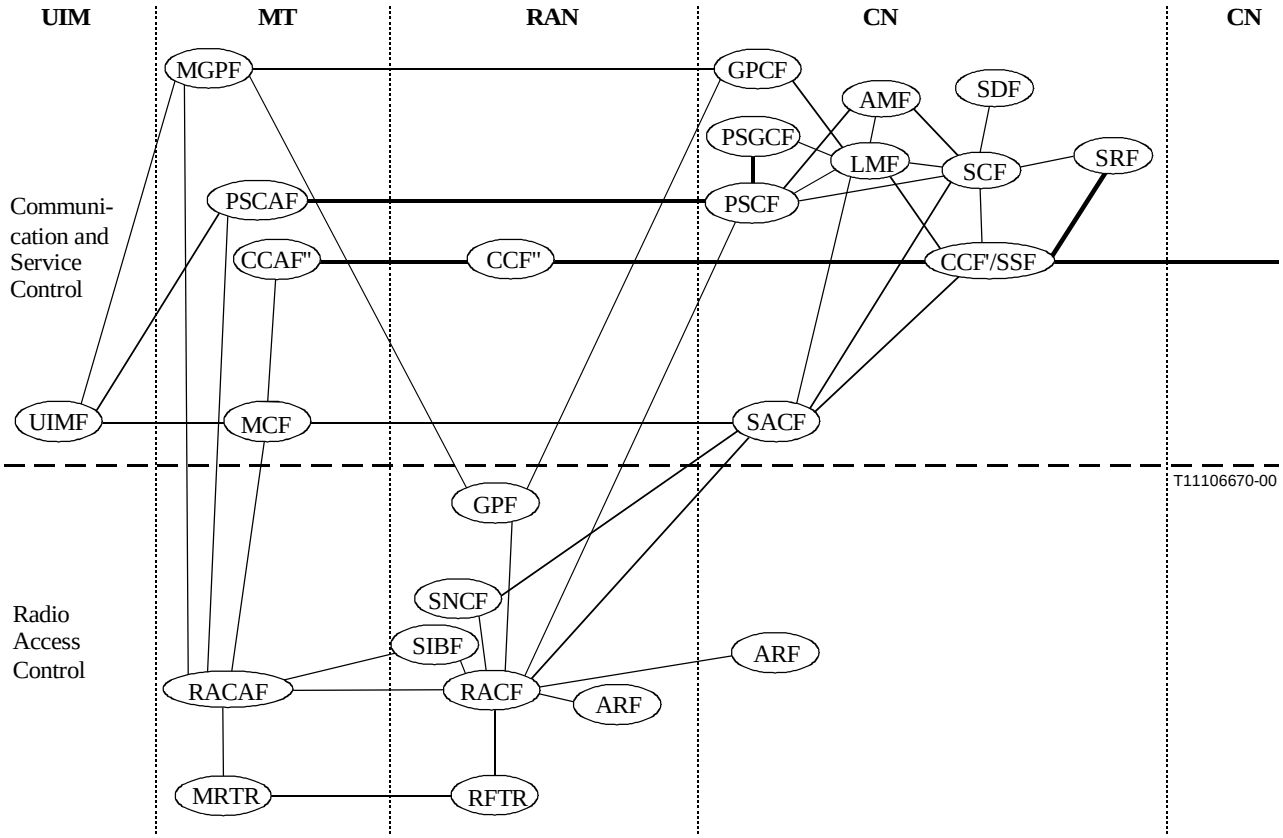
11.2 Choice of switching principles

The switching technologies (circuit switched, ATM, AAL2, frame relay, ...) shall be selected by the operator or service provider.

11.3 Call and Bearer Control functional communications

Figures 11-1 and 11-2 have been reproduced from ITU-T Recommendation Q.1711, extended to show the CN-CN interface.

The bold relationships fall – either fully or partially – within the scope of Call and Bearer Control Signalling.



NOTE – CCF" is introduced to address protocol conversion functionality (related to Call and Bearer Control) between MT-RAN and RAN-CN interfaces.

Figure 11-1/Q.1751 - The IMT-2000 functional model
Alternative 1: Integrated Call Control and Connection Control FEs

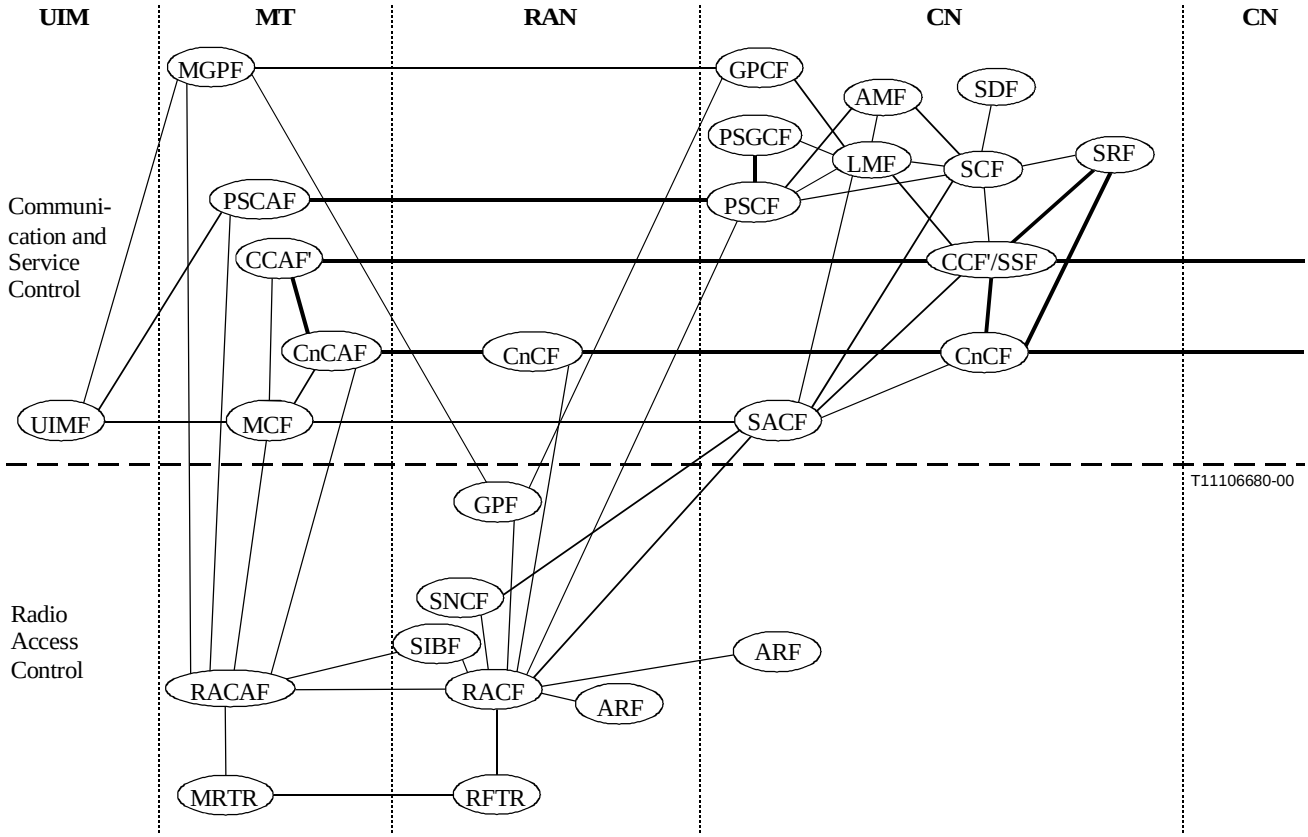


Figure 11-2/Q.1751 - The IMT-2000 functional model
Alternative 2: Separated Call Control and Connection Control FEs

11.4 Choice of Protocol Suite

The usage of the following protocols for IMT-2000 CS-1 are applicable:

Functional relationship	Protocol proposal
CCF'-CCF'	BICC N-ISUP for STM
CnCF-CnCF	Q.AAL2 for ATM AAL2 B-ISUP for ATM AAL1 NOTE – Others like PNNI/ATM or AINI/ATM are not excluded.

Due to timing constraints, the following functional relations have been assigned a lower priority within IMT-2000 CS-1 time-frame.

Functional relationship	Protocol proposal
CCAF'-CCF'	Family member specific protocol within the IMT-2000 CS-1 time-frame.
CnCAF-CnCF	
CnCF-CnCF	
PSCAF-PSCF	
PSCF-PSGCF	

Two domains have to be distinguished, the PSTN/ISDN-domain and the packet data domain as they pertain to the following protocols:

1) *ISDN/PSTN service domain*

   a) Call control: BICC, N-ISUP for STM;

   b) Bearer control: B-ISUP for ATM AAL1;
   Q.AAL2 for ATM AAL2.

   Flexibility is needed with respect to the IMT-2000 transport technology to meet the requirements of a deregulated, dynamic market.

2) *Packet data service domain*

   a) Call control: Not required.

   b) Bearer control: ATM AAL5 bearer.

   c) Network layer: Internet protocol (IP).

   Flexibility is needed with respect to the IMT-2000 transport technology to meet the requirements of a deregulated, dynamic market. Therefore different bearer types shall be allowed in IMT-2000 CS-1.

11.5 Multimedia calls

The IMT-2000 multimedia call requirements include the capability of merging the media streams on a single connection. The media are considered as different types of data streams (e.g. voice, data, image, etc.). These media can be multiplexed on a single connection and be controlled (e.g. adding, dropping media) by existing ITU-T Recommendations (e.g. H.323, H.245, H.248) operating "in-band" within the bearer connection. The requirement for AAL2 CS-2 is that the bandwidth of the AAL2 connection must be able to be modified. This requirement is addressed by AAL2 signalling CS-2.

11.6 Multi-party calls

The add/drop parties capabilities require only Point-To-Point communication configurations to a server or bridge (configuration 6), which can simulate the 2, 3, 4 and 5 configurations from a user's viewpoint. This Configuration Type 6 is a communication configuration that includes a server node (e.g. MultiPoint Communication Unit, MCU) within the network that can connect multiple Point-To-Point Connections. This will provide the end-user the possibility of MultiPoint-To-MultiPoint communications. The communication configuration Type 1 and 6 still allows for add/drop parties initiated by the root, leaf or third party (see TRQ 2001).

Furthermore, the multi-party call capability includes only the add/drop party capability initiated by the root or leaf. No third Party Add/Drop Party Capability is required for IMT-2000 CS-1. In addition to this, it is required to include the root notification signalling, when a leave initiated add/drop Party event occurs.

12 Protocol requirements for Packet Service Control

The functional elements that will support packet data services and their relationships across CN boundaries are shown in Figure 12-1. This clause identifies a set of requirements that pertains to NNI that supports the packet data services.

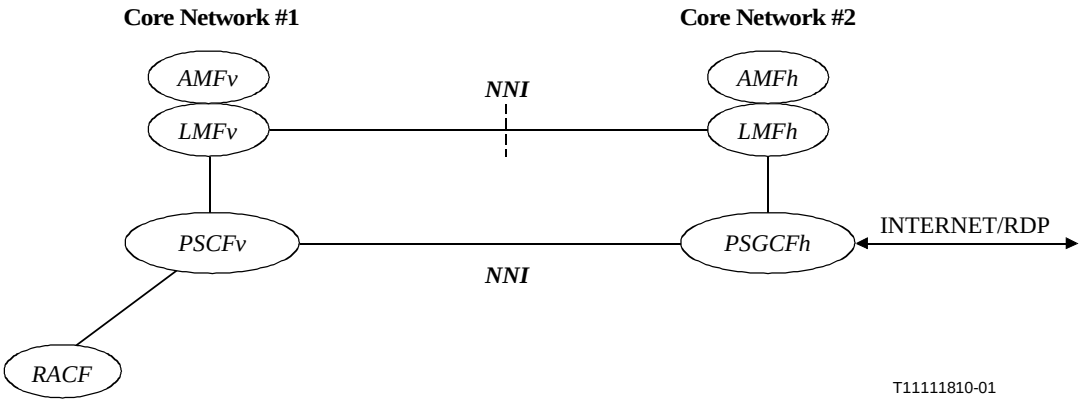


Figure 12-1/Q.1751 - Packet Data Network-to-Network Interfaces

12.1 The PSCF to PSGCF Interface protocol

The two functional capabilities that the PSCF and PSGCF will provide are:

1) transfer of user data between these two entities; and

2) interaction between these two entities for updates of packet service and routing contexts.

These two functions and the associated information flow belong to two disjoint logical planes: the user plane and the control plane. The first function identified above belongs to the user plane, while the second function belongs to the control plane.

The functional requirements listed below pertain to both the user plane and the control plane when the PSCF and PSGCF reside in two different Core Networks (CNs).

1) When the PSCF and PSGCF reside in two different CNs, these two entities should be interconnected over an IP network.

2) When the PSCF and PSGCF are connected over the public Internet, there should be a security association between the PSCF and PSGCF.

3) When the home CN authorizes the Mobile Terminal (MT) for data services in a visited CN, the home CN should instruct the visited CN to select either a specific PSGCF or propose allocation of a local PSGCF in the visited CN to handle a data service session.

4) When the data service session is established the allocated PSGCF should be fixed during the entire duration of the data service session. The visited core network in which this PSGCF resides becomes the anchor core network, CNa, for the data session.

5) When the MT initiates a data service session, the PSCF should be allocated by the CN where the data service session was initiated.

6) When the MT roams into a visited CN during an established service session, the visited CN should dynamically allocate a new PSCF to handle the respective service session. A succession of PSCFs may be allocated to the MT as it roams inside the visited CN (during the intra-CN roaming).

7) The IMSI or NAI may be used as a unique service-session identifier in all protocol transactions. If the MT supports several simultaneous service sessions, an associated Session Number identifier should be used to uniquely identify each individual service session.

12.1.1 User plane requirements

1) The PSCF and PSGCF should transfer the users' information over an IP network by employing a two-way IP tunnel.

2) The user plane may incorporate a mechanism that will support the concurrent existence of a multiplicity of two-way tunnel-connections inside the IP tunnel that connects the PSCF and PSGCF.

3) The user plane should incorporate an optional mechanism (e.g. encapsulation scheme) that will prevent out-of-sequence deliveries of users' packet data units across the tunnel-connection.

4) At any given time, each tunnel-connection between the PSCF and PSGCF should have a specified lifetime. The lifetime of a tunnel-connection should be extendible. Whenever the lifetime of a given tunnel-connection expires, the respective tunnel-connection should be cleared.

12.1.2 Control plane requirements

1) The control protocol between the PSCF and PSGCF should be able to establish individual tunnel-connections, extend the lifetime of the established tunnel-connections, and clear the established tunnel-connections.

2) The PSCF and PSGCF should employ the UDP to exchange control messages. These messages may be protected by an IP security tunnel.

3) A dedicated, well-known UDP port in the PSGCF should terminate a control channel over which control messages between the PSCF and PSGCF should be exchanged.

4) The PSCF and PSGCF should employ two-way (i.e. two-message) handshake protocol when establishing a tunnel-connection or extending the lifetime of an established tunnel-connection. The one-way protocol should be used to clear an established tunnel-connection.

5) The PSCF and PSGCF should be able to establish a security association with each other and perform encryption of data and authentication and integrity checking of control messages.

12.2 The LMFp to LMFp Interface Protocol

To access packet data services, the roaming MT will register with the visiting IMT-2000 network by employing common authentication and terminal registration procedures, and request access to packet data facilities. An associated accounting record may be kept to register the usage of packet data resources. The CN architecture should allow for separation of LMF (and associated AMF) capabilities that pertain to access facilities and LMFp (and associated AMFp) capabilities that pertain to the packet data services. The requirements listed below refer to the interaction between visited and home LMFps that reside in two different CNs and incorporate only the packet data capabilities.

1) When exchanging information that pertains to packet data services, the visiting LMFp and home LMFp should be able to convey the respective information over an IP network.

2) A security association between a visiting LMFp and a home LMFp should exist before information can be exchanged between these two entities. The security association may be automatically established, prearranged, or a visiting LMFp and a home LMFp can communicate through a trusted third party (e.g. broker) with whom they have, respectively, security association.

3) The protocol between the visiting LMFp (and associated AMFp) and the home LMFp (and associated AMFp) should enable the visited CN to authenticate and authorize the visiting MT to use the packet data services in the visited CN.

4) If the home LMFp fails to authenticate the MT, the visited CN will not allow packet data service. The visited CN will assume agreement for charging if the home network authorizes service.

5) When using packet data services, the visited MT may identify itself to the packet data network only with its NAI. The visited LMFp should be able to identify and locate the home LMFp based on the NAI.

6) The visited LMFp should be able to request, and the home LMFp should be able to identify the PSGCF that the visited CN should use for the respective packet data session.

7) The visited LMFp should be able to request, and the home LMFp should be able to supply an IP address that will be used by the MT during the respective packet data session.

8) The protocol between the LMFp peers should provide a mechanism to convey accounting information across this interface.

9) The LMFp peers should use a unique Session Identifier (Session ID) for each packet data session they mutually handle.

10) The LMFp peers should employ a set of Response Codes that should be included in every response message. The Response Code will provide reply information concerning the request (e.g. service denied, error condition, and bad password) to the requesting peer.

For packet data services, the IMT-2000 network will provide two levels of security – the access network security and the packet data network security. The access network security includes radio signal encryption and radio access key management for authentication of the MT. The packet data network security includes encryption and tunnelling of packets over the public Internet and authentication of the MT with the IMT-2000 network by using a secret key. The LMFp to LMFp interface requirements listed below pertain to the packet data network security.

1) For purposes of authentication and service authorization, the home CN may be able to provide security information regarding the MT to the visited CN.

2) A mechanism should exist by which the visited LMFp will be able to convey to the home LMFp the Challenge and Challenge response values. The Challenge value will contain the value that the visited CN passed to the visiting MT. The Challenge response value will contain the value that the visiting MT has generated using the Challenge value and the secret that the visiting MT shares with its home CN.

3) A mechanism should exist by which the visited LMFp and home LMFp will be able to exchange security parameters (e.g. SPI and security keys). The security parameters that were received from home LMFp will enable the visited CN to establish a two-way security association with the visiting MT, and between the PSCF in visited CN and the PSGCF in home CN.

APPENDIX I

Guidance on trigger concepts and usage

I.1 Purpose

The purpose of this informative appendix is to provide guidance on trigger usage through an informal discussion of some essential elements of trigger arming and processing within IMT-2000. It is expected that these basic guidelines will be further enhanced and optimized to fit the specific requirements (e.g. operational needs) of the different IMT-2000 family members.

I.2 Introduction

This appendix begins with a discussion of some principles and concepts. It then develops trigger usage and application guidelines based on these principles and concepts. Note that the principles and concepts, while based on the call related BCSM, are also applicable to the Location Management and Authentication State Models. The remaining subclauses of this appendix which discuss Dynamic Trigger Arming and Distribution of Triggers, require further consideration to determine whether these guidelines are appropriate for triggering Location Management and Authentication Management services.

Refer to IN ITU-T Recommendations Q.1231 and Q.1238 (Parts 1 and 2) for a further discussion on triggering and the BCSM call modelling principles on which the following subclauses are based.

I.3 Principles and concepts

1) Triggers are service independent:

   A fundamental concept of triggering is that triggers are service independent. This means that when an armed trigger is encountered and its criteria satisfied, the MSC does not know which service or services will be invoked as a result of the message it sends to the Service Logic Program (SLP) at the SCF.

2) Triggers include Service Logic Address Information:

   For the case of wireless subscribers, the service triggers, which implicitly indicates the SCF to be consulted, is located with the subscribers service profile located in the LMFh.

3) The SLP will respond with an executable instruction:

   The MSC expects that the SCF (SLP) will respond with an appropriate instruction on how to process the call. The MSC must consider the received instruction for appropriateness considering its current view of the call. In some circumstances, call-related events may have occurred between the query to the SCF (SLP) and the response from the SCF that make the instruction received inappropriate. One example is caller abandon.

4) Triggers are only acted upon when they are encountered in the BCSM:

   Some circumstances provide information earlier than when the BCSM looks for it. For example notification of Busy as a result of a mobility management procedure (e.g. location request). The O-BCSM model does not recognize this busy condition until call processing has progressed to a point where a T-BCSM is instantiated and the T-BCSM has progressed to the point where it encounters the T_Busy DP. If the busy status is not consumed there, the T-BCSM propagates it back to the O-BCSM for potential use there.

   Note that the discussion here describes the IN modelling (Refer to the Q.1238 series of ITU-T Recommendations). An implementation is free to consider the busy information as soon as it is available in order to optimize its performance, but must remain aware of the possibility of other services being invoked between the time when the busy information is received, and when the modelling indicates it should be considered.

5) Triggers take precedence in Order: Subscriber, Group, Office:

This sequence enables service providers to offer selected subscribers the use of services that are not available to the general subscriber base. Examples include access to enhanced services such as conference calling, etc. Similarly, this trigger precedence order allows service providers to deny selected subscribers services available to the general subscriber based. Examples include restricting calling parties to certain area codes, etc.

6) Each trigger is fully considered before the next trigger:

Triggers are listed in precedence order. This principle indicates that a given trigger type is considered for subscriber, group and office applicability before proceeding to the next trigger type in the precedence order.

It is possible to further refine items 5) and 6) to take into consideration precedence and sequencing of trigger criteria but this depends on the specific service and operational requirements of the particular IMT-2000 family member. For example, backwards compatibility with existing 2G systems may require specific handling of service triggers when operating in the context of 3G environment.

I.4 Dynamic trigger arming

A subscriber's trigger profile is stored with other service related information in the LMFh. This trigger profile is considered to be "static" because it changes slowly, if at all. That is, it remains the same unless the subscriber adds or deletes a triggered service from the profile, or turns on or off or modifies one of the services that are subscribed to. It is this "static" profile that is dynamically geographically placed as the subscriber roams and is served by different MSCs.

A subscriber's trigger profile may be modified for a given call instance without affecting the "static" profile. These modifications to the profile do not survive after the current call. On release of the call, all such modifications disappear. This is called "dynamic" trigger arming.

Dynamic trigger arming is a powerful capability. A powerful capability which can also be readily misused. It is incumbent on service providers using this capability to understand and deal with the potential side-effects of the use of this capability. For example, with multiple SCPs providing services, inappropriate use of the dynamic trigger arming capability may cause undesired service interactions or failures from the end-user's point of view. If not well coordinated, a service logic program on one SCP may overwrite triggers armed for a service logic program on another SCP. This may cause the other service to fail, or to not run at all, or to run incorrectly. With multiple service providers involved, they are unlikely to be aware of the full suite of services subscribed to and the effects they may have on these other, unknown-to-them services.

I.5 Distribution of triggers

Since wireless subscribers are inherently mobile, it is necessary to consider how the triggers for their services should be distributed. A mobile call origination or termination can occur anywhere and the roaming subscriber may be anywhere in the roaming areas available to the called mobile subscriber, it is necessary to distribute service processing in an optimal manner. It is assumed that when a service provider offers a set of services to a subscriber, the service provider should ensure that the services are an appropriate, coherent, and internally consistent set that will interact with each other in a manner desired by the subscriber.

The options for the dynamic geographic placement of statically armed originating and terminating triggers are at the Originating, Terminating or Gateway MSC. If identical trigger profiles are placed at the Originating, Terminating and Gateway MSC, then some services may be executed twice leading to undesirable results. Given that identical trigger profiles should not be placed everywhere, criteria are needed for use in deciding where to place triggers.

The following criteria is provided to assist the decision-making process to determine where to place the service triggers.

For optimization of network resources, outgoing call originating triggers should be placed as close as practicable to the calling subscriber. In general, this means that the subscriber's originating triggers should be placed at the originating MSC when the MS registers.

For calls to a subscriber, in order to ensure optimal use of network bearer connection resources, it is desirable to place triggers for services that may prevent call completion, as close to the originating point of the call as possible. Hence, a set of terminating triggers may be placed at the Originating or Gateway MSC for use in a BCSM being run as a proxy for the called subscriber. These triggers should be indicated in the information returned with the routeing (or location update) request. However, it should be noted that placing trigger profiles in the Local Exchanges (MSC) costs more and commits the network service providers to a higher cost deployment of the service before the market for the service is proven. Generally unless the Service requires high availability (high usage or low responses times) or requires deployment in the Local Exchanges (MSCs) for technical reasons the cost advantages to deployment in transit exchanges or interrogating gateways need to be considered.

If the call may be deflected to another destination, this should be done as close to the source of the call as possible (e.g. Originating or Gateway MSC). Service example is call forwarding to a voicemail service.

Security of Signalling may require that Triggers be deployed in a transit or a gateway node. Thus, if the SSF is in one network and the SCP is in a different network, STPs and GTT will be required at the signalling transport level. The use of STPs and GTT will reduce the speed of the signalling and will require extra security for the service providers to secure their protocol context.

High usage of a service requires it to be deployed in the visited MSC, Originating or Terminating.

The need for very short response times requires it to be deployed in the visited MSC, Originating or Terminating.

Networks which employ Optimal Routing may require triggers to be deployed in the visited MSC, Originating or Terminating, As triggering at the Interrogating (transit) node may cause complex routing, e.g. tromboned legs.

Signalling Timeouts may require that the originating triggers are placed in the Originating MSC and that the terminating triggers are placed in the Terminating MSC. Since, a number of specific conditions require the MSC to reset the ISDN short timeouts on the network access whilst the SCP is processing the application, this cannot be achieved at other exchanges.

Access to Location Area information may require that the originating triggers are placed in the Originating MSC and that the terminating triggers are placed in the Terminating MSC. This requirement may be alleviated by future signalling systems, which allow the LAI information to be relayed in the call path as CLI may be today. However, the screening of such parameters at network boundaries may render the signalling ineffective.

Home Network Applied Charging may require that Triggers be deployed in a transit or gateway node. Since if, the SSF is in one network and the SCP is in a different network. The Home network may never receive the call. Indeed it may be removed from the call path and so cannot secure the charging applied to the call. Other charging methods may require that service triggers are also deployed as close as possible to the called party. For example, services which require specific knowledge of radio interface parameters used such as, Cell ID, number of radio channels used etc., to ensure accurate calculation of charges. Other service examples include Mobile Terminating prepaid and Advice of Charge.

Local Area services will require that the originating triggers are placed in the Originating MSC and that the terminating triggers are placed in the Terminating MSC. For example, user exclusion or privileges on a base station. This may be the equivalent to line-based services in the fixed network.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems