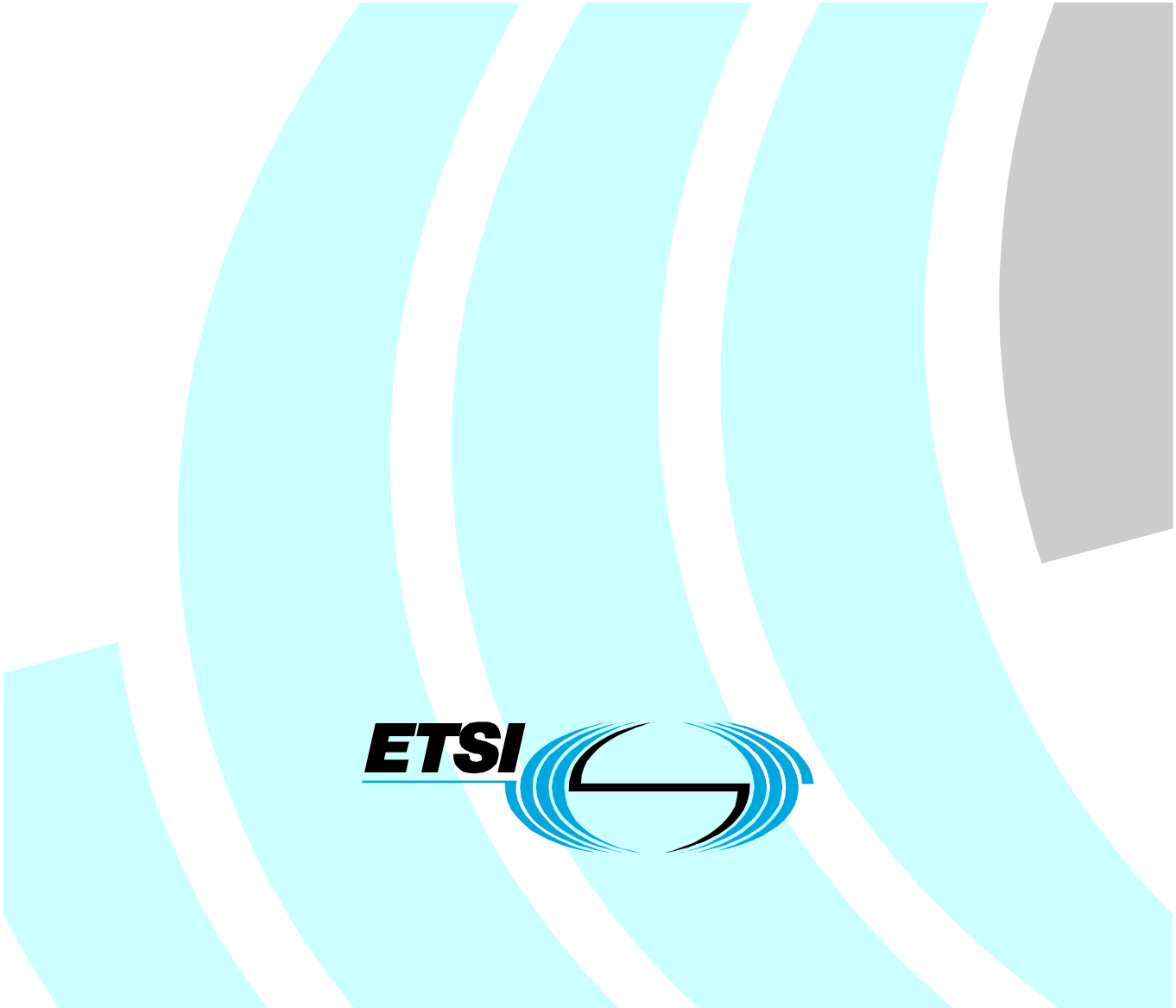
ETSI TS 101 315 V1.1.1 (2002-03)

Technical Specification

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Functional entities, information flow and reference point definitions; Guidelines for application of TIPHON functional architecture to inter-domain services



Reference
DTS/TIPHON-02007

Keywords
architecture, internet, IP, service

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2002.
All rights reserved.

Contents

Intellectual Property Rights 5
Foreword 5
Introduction 6
1 Scope 8
2 References 8
3 Abbreviations 9
4 Introduction 9
4.1 Structure of the present document 9
5 TIPHON meta-protocol 10
5.1 Introduction 10
5.2 Example: Information flows for a call set-up in TIPHON abstract architecture 14
6 Registration 15
6.1 General structure 15
6.2 User at home scenario 15
6.2.1 Simple form: Attachment only 16
6.2.2 User registration 17
6.2.2.1 Verification 17
6.2.2.2 Authentication 17
6.2.2.3 Service attach notification 17
6.2.2.4 Ticket generation 18
6.2.2.5 Response to terminal 18
6.2.2.6 Attachment with SpoA 18
6.2.3 Single sign-on service 18
6.2.4 De-registration 18
6.3 Roaming user scenario 18
6.3.1 Relationships for roaming case 19
6.3.2 Registration with RpoA 20
6.3.2.1 Example 20
6.3.3 Service attachment with (proxy) SpoA 20
6.3.4 De-registration 20
7 Simple call applications and services 21
7.1 Simple call 21
7.1.1 Initiating the call 21
7.1.2 Clearing the call 23
7.2 Simple call with ICF 23
7.3 Support for intra-domain QoS 24
7.4 CLIP/CLIR 25
7.5 Event recording 27
7.6 Lawful interception 27
7.7 IP and SCN interworking 28
7.8 VoIP interconnect 29
7.8.1 VoIP interconnect with an example of IP address translation 30
7.8.2 VoIP interconnect with an example of QoS 31
7.9 Roaming User scenario 32
7.10 Number portability 34
7.10.1 Number portability - All Call Query 34
7.10.2 Pivot routing 35
7.10.2.1 Call drop-back 35
7.10.2.2 Onward routing 36
7.10.3 Query on Release (QoR) 37
7.11 Priority Calls 38

7.12 Emergency Calls 39
7.13 Carrier Selection....40

Annex A (informative): Bibliography....41

List of figures....42

History....43

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

Introduction

Figure 1 shows the relationship of the present document with other TIPHON Release 3 deliverables.

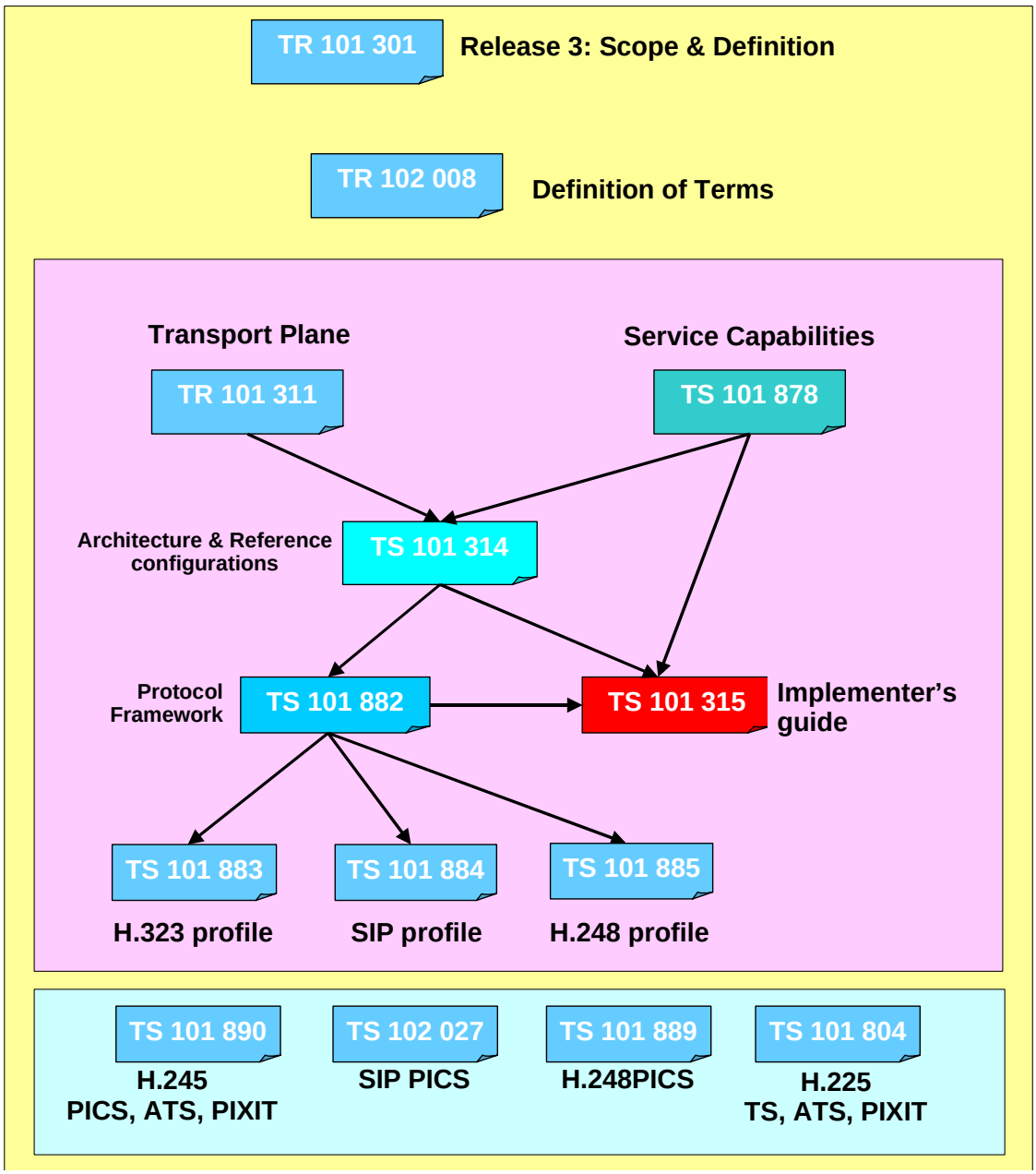


Figure 1: Relationship with other TIPHON Release 3 documents

- TR 101 311 [8] provides the requirements on the transport plane,
- TS 101 878 [1] defines service capabilities that are used in the TIPHON Release 3 for a simple call,
- TS 101 882 [3] provides the protocol framework based on the TIPHON Release 3 architecture to implement the simple call service capabilities as defined in the present document,
- TS 101 315 (the present document) is an implementer's guide that shows how to use of the meta-protocol to realize the capabilities as defined in TS 101 878 [1].
- TS 101 883 [4] provides the protocol mappings for the ITU-T H-323 profile,
- TS 101 884 (see bibliography) provides the protocol mappings for the SIP profile,

- TS 101 885 [5] provides the protocol mappings for the ITU-T H-248 profile,
- TS 101 314 [2] provides the architecture and reference configurations for TIPHON Release 3.

1 Scope

The present document describes how the generic information flows as specified in the TIPHON baseline architecture [2] and meta-protocol [3] will be used to specify certain inter-domain service capabilities, as required in TS 101 878 [1].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] ETSI TS 101 878: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Capability Definition; Service Capabilities for a simple call".

[2] ETSI TS 101 314: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; abstract architecture and Reference Points Definition; Network Architecture and Reference Points".

[3] ETSI TS 101 882: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Protocol Framework Definition and Interface Requirement Definition; General (meta-protocol)".

[4] ETSI TS 101 883: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology Mapping; Implementation of TIPHON architecture using H.323".

[5] ETSI TS 101 885: "Telecommunications and Internet protocol Harmonization Over Networks (TIPHON) Release 3; Technology Mapping; Implementation of TIPHON architecture using H.248".

[6] ETSI TR 101 301: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Release Definition; TIPHON Release 3 Definition".

[7] ETSI TR 102 008: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Terms and Definitions".

[8] ETSI TR 101 311: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Independent requirements definition; Transport Plane".

[9] ETSI TS 101 520: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Implementation Conformance Statement (ICS) proforma for the support of packet based multimedia communications systems; Support of ITU-T Recommendation H.323".

[10] ETSI TS 101 521: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Protocol Implementation Conformance Statement (PICS) proforma for the support of call signalling protocols and media stream packetization for packet-based multimedia communication systems; Support of ITU-T Recommendation H.225.0".

[11] ETSI TS 101 522: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Protocol Implementation Conformance Statement (PICS) proforma for the support of control protocol for multimedia communication; Support of ITU-T Recommendation H.245".

[12] ETSI TS 101 804 (all parts): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology compliance specifications".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ACQ	All Call Query
APCS	Authorized Priority Call Service
BC	Bearer Control
BICC	Beraer Independent Call Control
CC	Call Control
CDR	Call Data Records
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CR	Call Routing
FG	Functional Group
ICF	Isochronous Convergence Function
IMP	Instant Messaging and Presence
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
MC	Media Control
MSC	Message Sequence Chart
NAT	Network Address Translation
NNI	Network-to-Network Interface
NWFG	NetWork Functional Group
QoR	Query on Release
QoS	Quality of Service
QoSPE	QoS Policy Element
RAS	Registration Admission and Status
RPoA	Registration Point of Attachment
RTP	Real Time Protocol
SC	Service Control
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLA	Service Level Agreement
TPE	Transport Policy Entity
TRM	Transport Resource Manager
TU	Transport Usage
UNI	User-Network Interface
VoIP	Voice over IP

4 Introduction

The present document is intended to provide the users of TIPHON specifications with guidelines on their usage for specific scenarios.

4.1 Structure of the present document

Clause 5 gives an overview of the meta-protocol role as defined in the TIPHON process [3]. The remainder of the flows in the present document are expressed in terms of this meta-protocol. Readers interested in the implementation of a scenario described in the present document are encouraged to read the technology mpping documents dealing with each individual technology mentioned in the present document. See TS 101 883 [4], TS 101 884 (see bibliography), TS 101 885 [5] and DTS/TIPHON-03028R4 (see bibliography).

The TIPHON registration method is described in clause 6.

In clause 7 several call scenarios are described. The services being referred to in [1] are:

- Simple call setup,
- Simple call setup with ICF,
- Support for Intra-Domain QoS,
- Support for CLIR/CLIP,
- Billing,
- Lawful Interception,
- SCN Interworking,
- VoIP domains Interconnect supporting NAT,
- VoIP domains Interconnect supporting Inter-domain QoS,
- Roaming,
- Number Portability,
- Priority Calls,
- Emergency Calls,
- Carrier Selection.

5 TIPHON meta-protocol

5.1 Introduction

The telecommunications industry has a long tradition of creating specialist protocols for individual services. Often several flavours of one protocol were used or several protocols existed to address the same problem. From an interworking perspective these multiple protocols represent a significant challenge, because each of them assumes that messages and code points are available to define the service. The consequence is that the service definition is different on either side of an interworking point, often only in a subtle way. This means that interworking is a complex problem involving a large number of compromises. More specifically, if there are *n* protocols to inter-work then there are *n x (n-1)* interworking approximations that need to be developed.

TIPHON Release 3 introduces the use of a meta-protocol to manage the overall complexity to achieve multi-protocol interworking. As shown in figure 2, the process of interworking is defined in terms of rules for encoding the code points, mapping the messages and modifying states. As a consequence, the number of interworking approximations is reduced to *n* rather than *n x (n-1)*. A TIPHON service application is therefore defined in meta-protocol terms rather than with any other protocol used at the point of interworking. A mechanism is then defined for interworking with each desired, or candidate protocol. Hence a mapping to and from the meta-protocol (designed to support the services needed) is defined for each concrete protocol to be used. This mapping must also take into account the behaviour of underlying transport layers and protect against message loss. The derivation of these mappings is a complex task. However, it is not always possible to apply the meta-protocol to generate a complete mapping to a given protocol. This either results in writing new meta-protocol extensions or in deficiencies in the chosen concrete protocol.

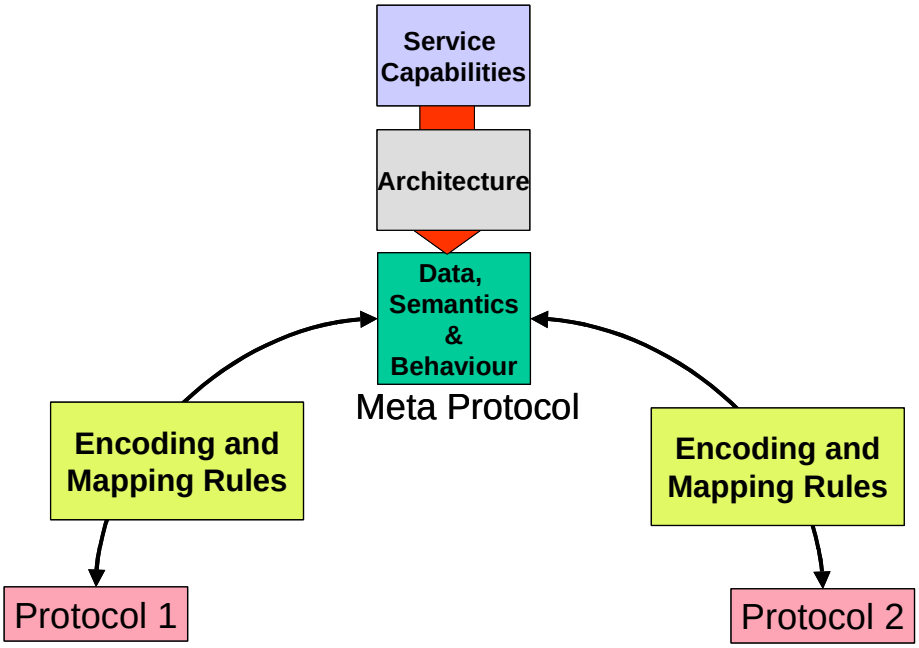


Figure 2: Meta-protocol enabled interworking

More formally, the TIPHON meta-protocol is an application level functionality, which encompasses a whole host of applications required for next generation telephony. It provides a super set of capabilities to support the telephony application, in a protocol and transport technology independent way. The meta-protocol consists of call state machines, which can perform the call processing. Different standard (and non standard) protocols can be mapped to this superset functionality to provide interworking between them. It can be implemented in its entirety to develop communications application servers, or it can be used as a tool to enhance existing protocols and to provide interworking between them.

The basis of the meta-protocol is the TIPHON abstract architecture, which defines functional layers, reference points and interfaces between the functional layers. (See [2] for a full definition of this structure.) A functional layer performs a specific set of tasks, e.g. the Call Control functional layer performs call processing; the Bearer Control functional layer performs bearer setup/negotiation, etc. A set of these layers forms a functional group.

TIPHON architecture defines five layers of functionality, which are:

- Service layer,
- Service Control layer,
- Call Control layer,
- Bearer Control layer,
- Media Control layer.

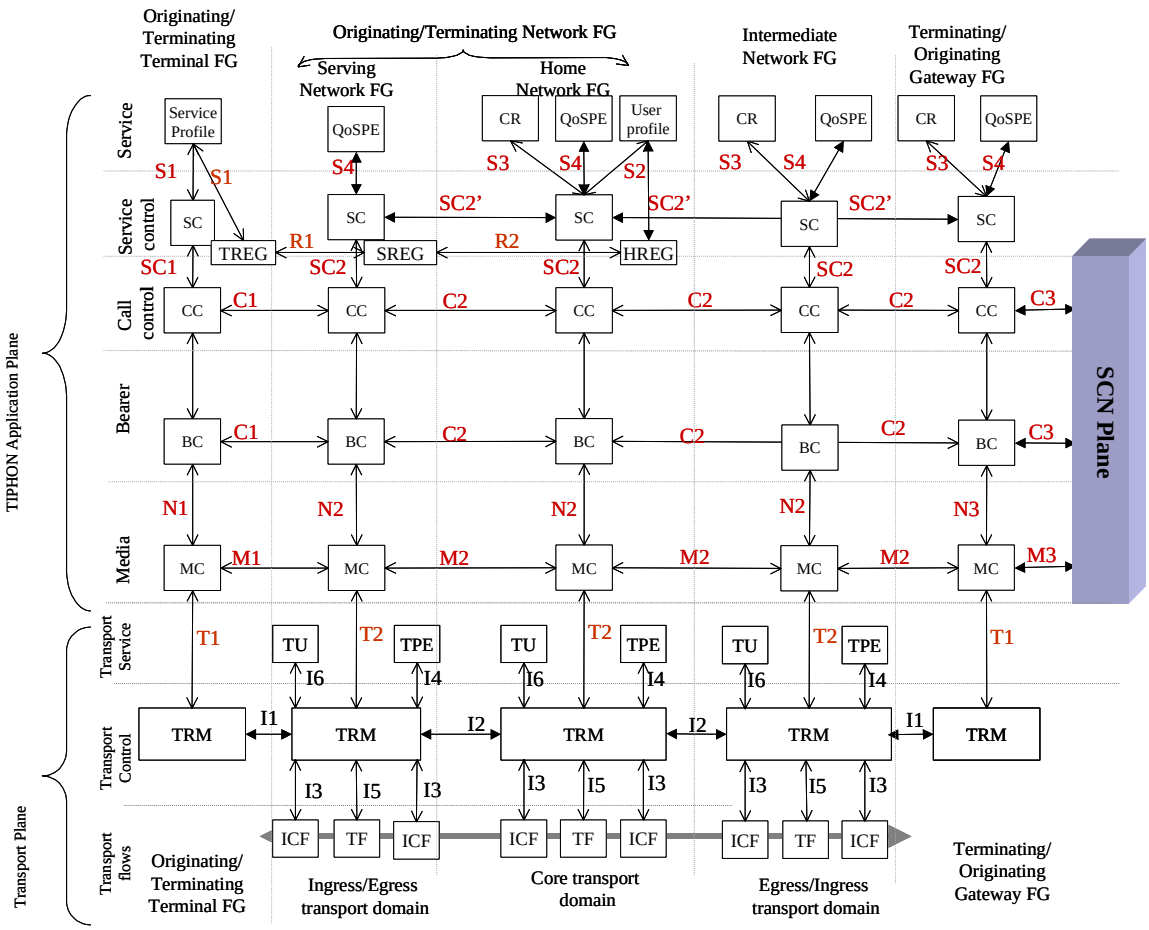


Figure 3: TIPHON application architecture

Figure 3 shows an example of TIPHON architecture, FGs and reference points for the applications.

For the whole system to work, each functional layer carries out a set of tasks, and communicates information requests and responses, to other functional layers. This flow of information takes place on reference points bothvertically and horizontally.

This abstract architecture can be mapped to real "boxes", e.g. The CC and BC layers map to a NWFG (e.g. a SoftSwitch, SIP B2BUA, H.323 gatekeeper); the Service layer could map to a Registration Server, or a Parlay Server. The information flows between these functional layers take place at reference points in the form of real protocols, e.g. the C reference point could be supported by H.323, SIP, BICC, ISUP etc; the N reference point could be supported by the Megaco/H248 protocol.

But all the above standardized protocols behave differently, are technology dependent, and do not always allow a seamless service interworking. Also, these protocols do not fulfil the requirements of all the reference points. The meta-protocol was developed to encompass the behaviour and context of all the functional layers into one set of functionality.

Some of the services provided by the meta-protocol are given below:

- Registration of subscribers,
- Authentication of users,
- Authorization of services,
- Provide services in home or visiting network (roaming),
- Call Control functionality,
- Call setup/teardown/call management,

- Bearer Control functionality (departure from the old monolithic CC functionality, as the bearer is no more tied tightly to the Call Control):
  - Bearer setup/teardown/management,
- Aggregate bearer:
  - (old trunking facility in packet networks),
- Service control/access/provision:
  - Access to switch based and non switch based services,
- Media control functionality, to manage different types of media, having different attributes,
- Provides all of above for multimedia sessions.

There are several parts of the meta-protocol, which refer to the TIPHON reference points they support, hence, the type of services those reference points provide. The reference points supported by the meta-protocol are:

Table 1: Mapping of Reference points to target protocols

Reference point	Purpose	Candidate protocols
R	Registration	
C	Call Control	SIP, H.323, BICC, ISUP
BC	Bearer Control	SDP, H.245, BICC-SDP
M	Media	RTP
N	Media Control	MEGACO/H.248
T	Transport Control	MEGACO/H.248 + EMP (TS 101 332)
S	Services (access to)	
SC	Service Control	INAP, Parlay, OSA, JAIN, SIP

There are sub parts of the above reference points, e.g. the C reference point consists of C1, C2 and C3. Each of these subparts carry slightly different information since they operate between functional groups with a different role in call processing, but provide the same type of service: Call Control signalling.

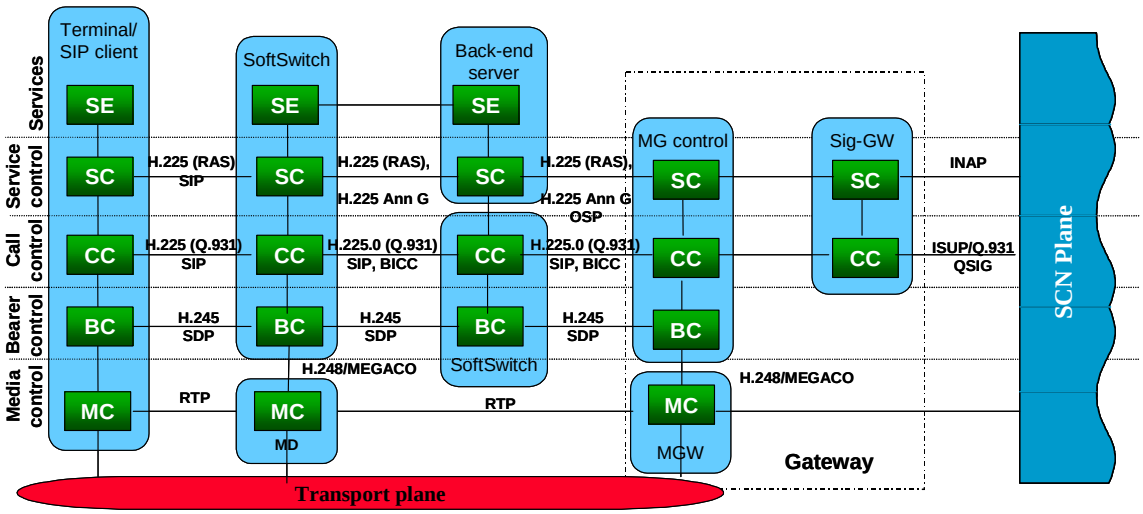


Figure 4: Example implementation of TIPHON architecture

The reference points listed in table 1 can be used as guidance of what capabilities need to be supported in an open VoIP system. Standard protocols, such as SIP, H.323, BICC, Megaco, can be mapped to these reference points for secure and QoS enabled intra-domain and inter-domain communications. Figure 4 shows the placement of the standardized protocols on TIPHON abstract architecture.

The mapping to standard protocols allow the implementation of the TIPHON system according to the choice of technology (protocols) of a vendor or service provider. Because TIPHON specifies the mapping of individual technologies (protocols) to the meta-protocol, it means that interworking these protocols via the meta-protocol is an automatic result.

The service capabilities supported by TIPHON meta-protocol can be used to develop standard or operator specific services, allowing for "innovation for revenue generation". These standard service capabilities supported by TIPHON R3 are based on the requirements study [1].

For example, a service provider deploying H.323 can Interconnect with a service provider deploying SIP, or BICC; or even support customers on its network with devices using different protocols. If this service provider needs to interconnect with a network that uses a different technology, an entity is needed that provides the service of this provider over that technology. The TIPHON approach allows this service provider to express the service in a technology independent way and purchase entities that provide this service over any applicable technology. Also if a technology is implementing a service in a way that is compatible with the TIPHON mapping, protocol conversion is made easier because the underlying state machines of both implementations can be linked to the state-machine of the TIPHON meta-protocol.

5.2 Example: Information flows for a call set-up in TIPHON abstract architecture

The Functional entities in the TIPHON can communicate with each other using the meta-protocol. The information flows can be Horizontal and Vertical, as shown in figure 3. This clause shows an example of a Simple Call set-up between two terminals, as well as the information flow that takes place between different Functional entities, such as Call Control (CC) and Service Control (SC). This example concentrates on call flows only in the TIPHON Application.

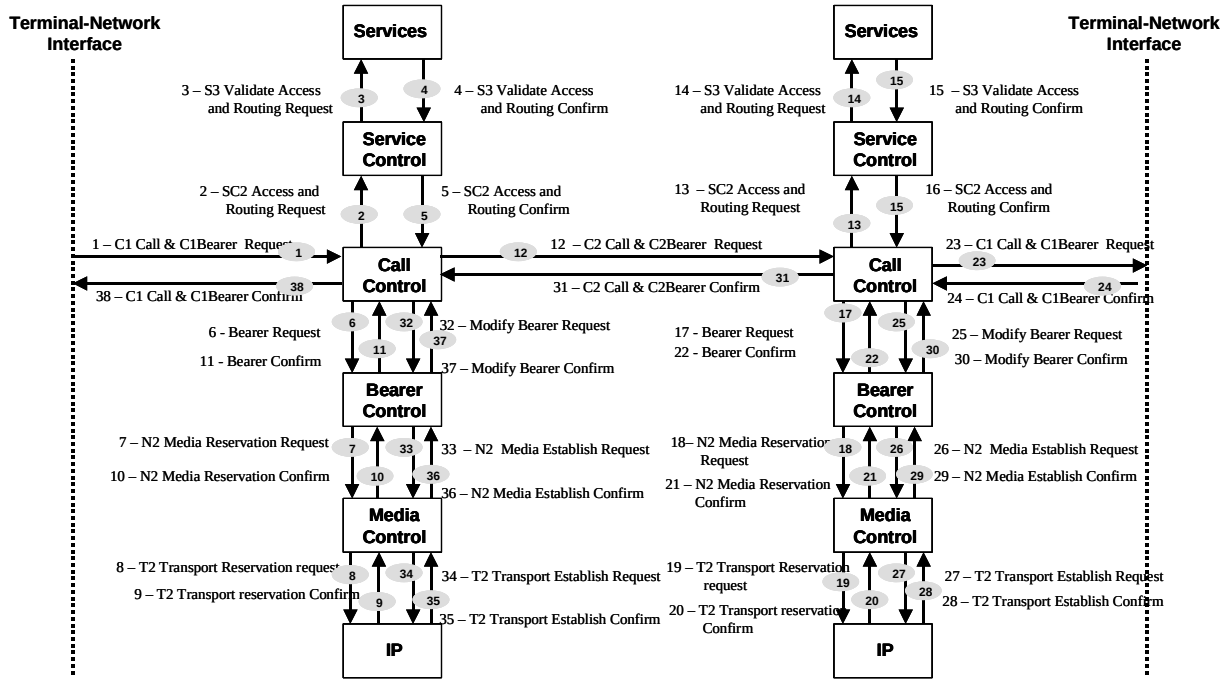


Figure 5: Call set-up using meta-protocol

Figure 5 shows the sequence of events that takes place in a simple call set-up. The message prefixes, e.g. C1, T1, refer to the information flows that take place on the corresponding reference points: C1 reference point, and T1 reference point.

It is envisaged that it can be difficult for the reader to follow the events taking place in the functional entities, and subsequent information flows vertically and horizontally in the TIPHON application plane. Therefore, the call flows in the rest of the present document utilize the Message Sequence Charts (MSC), to show how the meta-protocol supports the services as defined in TS 101 878 [1].

6 Registration

In the TIPHON service-model, a user has a contract with one (or more) service providers. Prior to using the service, the user shall attach to the service node that provides the service. The service node that shall be used for a particular invocation of the service may be known a-priori or may be selected dynamically, based on the context like user location, user permissions and preferences and load-sharing.

6.1 General structure

The registration service allows a user (registrant) to register with a registrar. The registration service includes the authentication and authorization of a subscriber (user/registrant) to access a service. It is a pre-requisite: a successful registration would normally lead to access services which the user is entitled to use; whereas, an unsuccessful registration would normally lead to refusal of service. The latter may however not apply in certain cases, e.g. accessing emergency services.

In figure 6 an overview is given of the basic registration mechanism.

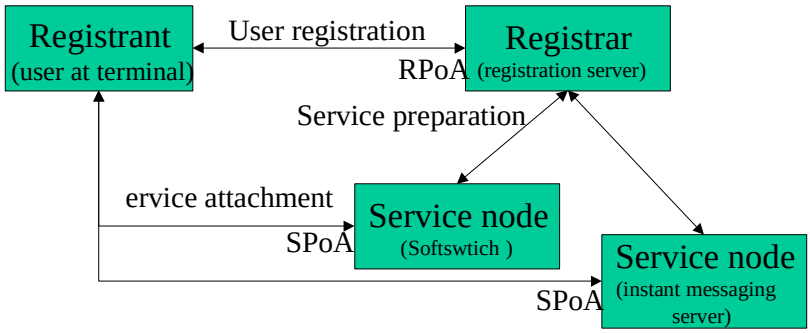


Figure 6: General structure of the TIPHON registration mechanism

1) User registration: The user registers for the service and shows entitlement for the service used.

2) Service preparation: The registrar selects a service node at which the user shall use the service and informs the service node that the user is entitled to use the service.

3) Service attachment: The user (terminal) attaches to the service node and the service can be delivered.

TIPHON has developed a registration meta-protocol which defines the context, procedures and behaviour of the Registration service. This registration meta-protocol can be mapped to standard protocols such as SIP, or RAS (H.323). The TIPHON architecture identifies two reference points for registration: R1 and R2. R1 supports UNI and R2 supports NNI.

Two registration scenarios shall be supported:

- the "User at home" scenario; and
- the "Roaming user" scenario.

6.2 User at home scenario

The NORMAL "User at home scenario" registration process involves the following steps:

- registrar discovery;
- registration with registrar;
- registration with application server.

The complete procedure is not necessary for all deployments. We start with the simplest scenario and add functionality upon that.

Before any kind of registration takes place, a user/terminal needs to know who the registrar is, who to register with. In the simple case the signalling handle on the registrar (the RpoA) can be provisioned in the terminal.

However TIPHON allows for a dynamic discovery mechanism. The details of this mechanism are outside the scope of TIPHON Release 3.

6.2.1 Simple form: Attachment only

In its simples form the user at home scenario can default to simply the service attachment. The user may have been provided with a username and password and/or a suitable cryptographic key that will prove the user's right to access the service. Also in the simplest form, there is just one service node or the user terminal can select one on its own.

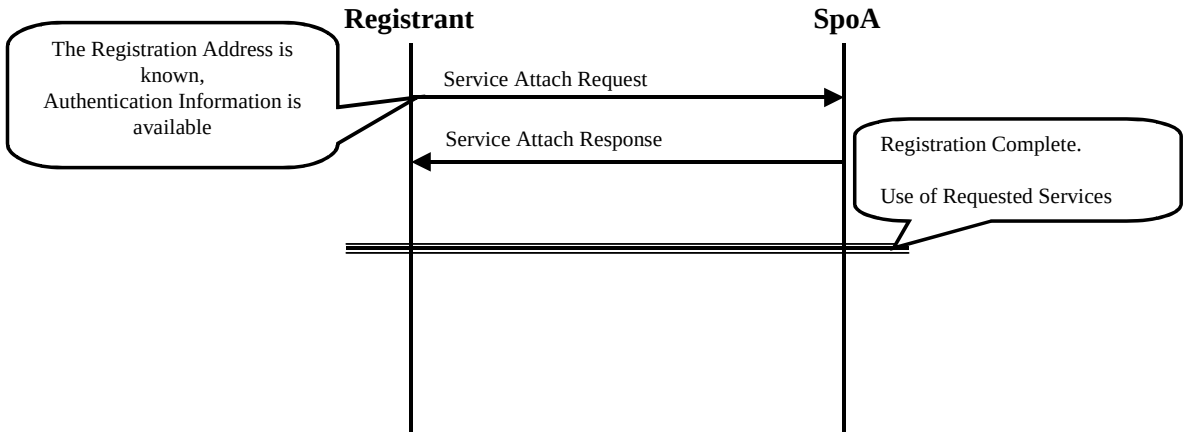


Figure 7: Service attachment

In figure 7, a simple service attachment is shown. The user provides credentials that give it entry to the service (may be *null* for an anonymous service) and may provide details of the service desired (may be *null* if there is only one service provided at that node). This information is sent to the address of the service node (SpoA, Service point of Attachment). The service node stores the relevant data, acknowledges to the user.

When the user is no longer interested in the service, the user (terminal) may detach from the service as is shown in figure 8.

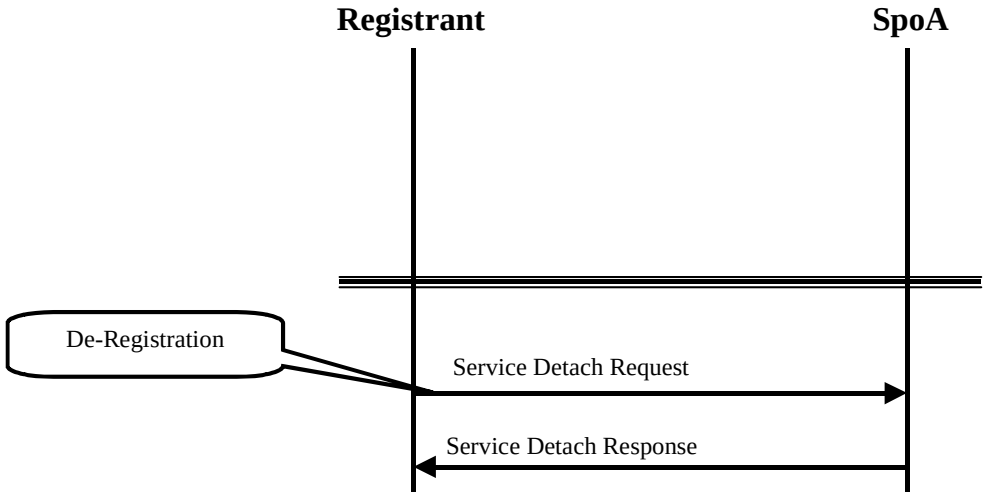


Figure 8: De-attachment

After this detachment, the user must re-attach if further service is required.

6.2.2 User registration

Requiring that users register prior to service attachment is a more flexible and secure method.

Once the identity of the registrar and its signalling handle RpoA is known, the next step is to register with it using a registration protocol. It is, however, important at this stage to clarify the difference/commonality between the RpoA and registration server. RpoA is the access interface to a registrar. It may or may not be co-located with the registration functional grouping. There may be a case when an RpoA serves as a Registrar location server, receives registration requests, and provide the address of a relevant registration server. For simplicity, we consider a case where RpoA is the registrar (co-located with the registration functional grouping).

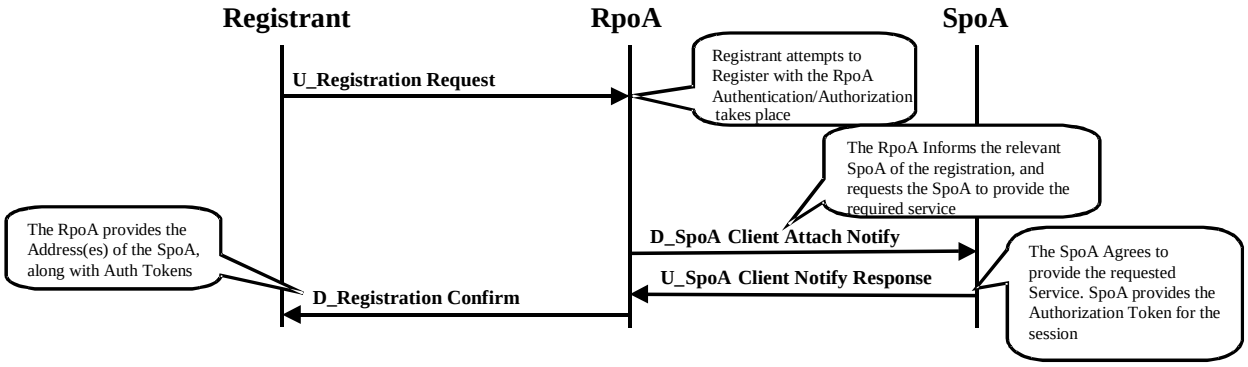


Figure 9: Simple user registration

The user registration scenario is shown in figure 9.

It is a four step process in which the terminal (user) initiates Registration by sending a "Registration Request" message to the RpoA. Using the Registration Request message to the RpoA (Registration point of Attachment), the user is identified to the registrar. This message may also carry the request for services the user wants to use. If no services are mentioned, the registrar assumes that all services the user is entitled to are requested.

Upon receipt of this message, the following procedure takes place at RpoA.

6.2.2.1 Verification

The user is verified as a subscriber based on the Public identity he provided in the Registration Request. This verification could involve communications between the RpoA and a database. The communication with the database is outside the scope of TIPHON Release 3.

6.2.2.2 Authentication

Authentication takes place to check that the user is what he claims to be (via Public id). The RpoA checks for the authentication information in the Registration Request message. If the authentication information (combination of private id and password) is not available, the registration request is declined. The user then sends another registration request with appropriate authentication information (in a secure manner - to be discussed later).

6.2.2.3 Service attach notification

After success authentication, the RpoA checks the services requested by the Registrant. This could involve matching the requested services with a local (to registrar) service profile. This step is outside the scope of the present document.

The registrar selects a service node(s) that shall host the service for the user and notifies this node that it shall serve as this role. The RpoA searches for the possible application servers (telephony, IMP, etc) that can provide the services requested by the registrant. Once found, the RpoA communicates with the relevant Application Server(s), SpoA, to inform them of the client registration, via "Client Attach Notify" message. The SpoA then either accepts or rejects to provide the requested service (possibly based on available resources).

6.2.2.4 Ticket generation

If the SpoA accepts to provide the requested service, it replies with a "Client Attach Response", including a ticket that can serve as an authentication token. The service node acknowledges this and provides the RpoA with a ticket that can be passed to the user.

6.2.2.5 Response to terminal

The registrar collects all the tickets from all the nodes it contacted and acknowledges the registration and presents the users with the tickets. Using this ticket the user can later show entitlement to the service nodes using the service attachment procedure as shown in the following clause.

6.2.2.6 Attachment with SpoA

Once the registration with RpoA is completed successfully, the User then registers with the SpoA. SpoA is a service point of attachment, and may provide one or more services. The examples of services provided by SpoA include, but not restricted to: Voice over IP, Instant Messaging, etc. Note that there may be more than one SpoA (in different service providers domain) providing these services.

The registration with the SpoA is achieved by sending a "Service Attach Request" message to the SpoA. This message contains, amongst other data, the ticket provided by the SpoA to the RpoA, via "Client Attach Response" message, and then to the registrant via "Registration Response" message. This token confirms that the user is authenticated to utilize service(s) provided by the SpoA.

NOTE: For security reasons the ticket is valid for a defined period of time.

6.2.3 Single sign-on service

The above steps for registration show that the registration service in effect requires registration with two entities, RpoA and SpoA. In simple cases these nodes may be the same. They have been modelled as separate nodes because it is envisaged that next generation networks will provide multiple services instead of just telephony, and these services may be provided by different servers, or even different service providers. The multiple services may include Instant messaging, presence services, video conferencing etc. The philosophy behind the registration with the RpoA is that there should be one point of attachment where a user registers for all the services it wishes to use. This saves the user from having to register and authenticate for services with each of the application servers: the RpoA does it on the user's behalf.

6.2.4 De-registration

The registration is valid only for a specific time period, after which it expires. If the user/registrant wishes to continue using services, or being registered, it needs to re-register before the registration expires. If no Re-registration is carried out, it is assumed that the user does not want to continue to be registered, and is implicitly de-registered at the registration expiry timer.

If the user wants to explicitly de-register from all the services/servers, it sends a de-register request to the RpoA. The RpoA then notifies all the SpoAs of the client detach. There is a possibility that the client only wishes to de-register from a specific SpoA. It then issues a "U-SpoA Service Detach Request" to the relevant SpoA. See figure 10 for call flows.

6.3 Roaming user scenario

This is a scenario where a user is roaming in a visited domain. No assumption can be made about prior knowledge of the addresses of the RpoA or SpoAs. The registration procedures, however are similar to those covered in the above clauses.

6.3.1 Relationships for roaming case

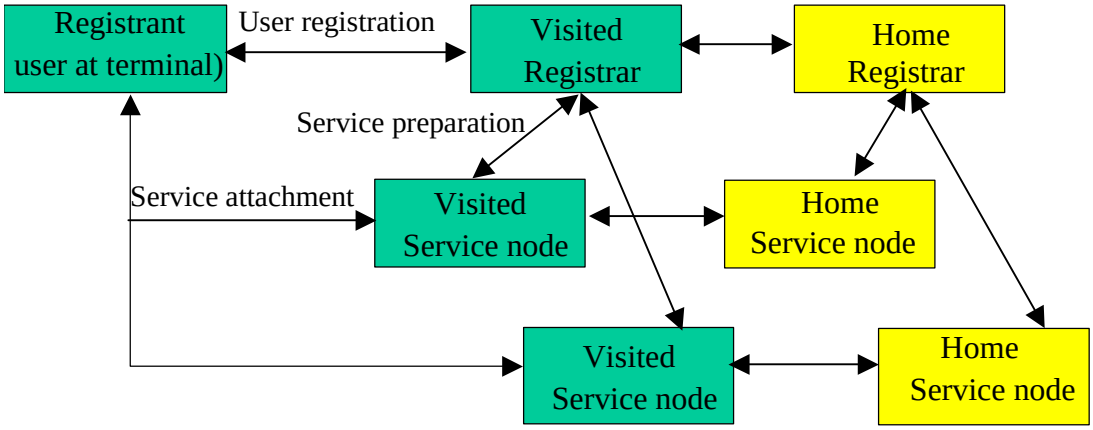


Figure 10: Roaming architecture

In this scenario it is assumed that a business relationship (SLA) exists between the home service provider and the visiting domain that will entitle the user to receive services in the visiting network.

The relationships are shown in figure 10. The user discovers the serving registrar in the visited domain just as it would discover the registrar in the home domain. The visited registrar contacts the home registrar and establishes service entitlement. TIPHON assumes that the services rendered can be unique and may not necessarily be provided by a party different from the home network. Therefore, for some services, the visiting network only provides a proxy for the service signalling and relays all the signalling to the home network.

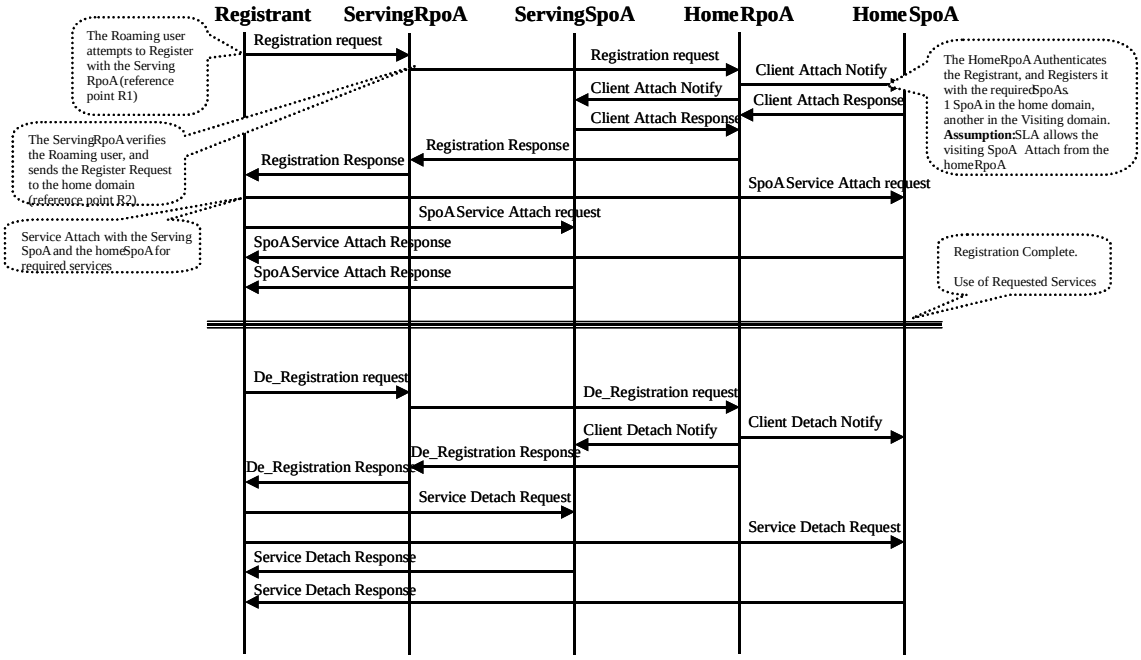


Figure 11: Full roaming sign-on scenario

The detailed roaming user registration scenario is covered in the following clauses, and shown in figure 11. This figure shows a registrant contacting a local RpoA (after first having discovered it).

The visited domain's RPoA then contacts the home registrar to establish the service entitlement of the user.

6.3.2 Registration with RpoA

Once the address of the serving RpoA in the visiting domain is known, the roaming subscriber sends a Register Request message to it. This information flows on TIPHON R1 reference point [2]. The serving RpoA identifies the Registrant as not belonging to its domain; but to a domain it has a SLA with (this is done possibly by some database query). If the serving RpoA does not have a valid SLA with the registrant's home service provider, the Registration request is declined, with the appropriate "Reject Reason".

If the registrant's home service provider has a valid SLA with the serving RpoA, then the Serving RpoA contacts the Home RpoA by sending a Registration Request message. This information flows on the TIPHON reference point R2.

The home RpoA receives the Registration request, Authenticates the Registrant, and checks if the Registrant has subscribed for roaming service. If he has, the RpoA then checks if the Registrant is allowed the requested services. If it is, the RpoA then checks which of the requested services need to be provided by the Serving domain (provided the serving domain can provide those services - a check based possibly on SLA); and which services are to be provided by the home domain. The next step is to identify the relevant SpoAs in both the home and visiting networks.

Once the target SpoAs are identified, the home RpoA informs the SpoAs of the Client attachment, via "Client Attach Notify" message. Upon successful notification, the SpoAs will return authentication tokens to the home RpoA. The RpoA will then send these tokens along with the SpoA Ids to the Registrant in the Registration Response message, via the serving RpoA.

6.3.2.1 Example

Consider a scenario where the Roaming Registrant requests two service: VoIP and Instant Messaging and Presence (IMP). The Home RpoA decides that the IMP service has to be provided at home, it will hence register the registrant with the home IMP server, and upon successful registration (with the IMP server), it will return the SpoA ID and authentication token to the Registrant in the Register Response message, via serving RpoA. The home RpoA also checks if VoIP can be provided by the serving domain, and (if yes), what is its VoIP SpoA ID. The home RpoA then registers the Registrant with the serving domain's VoIP SpoA, receives authentication token, and send the SpoA ID and token to the Registrant in the Registration Response message.

6.3.3 Service attachment with (proxy) SpoA

After the successful registration with home RpoA, the next step is to register for services with relevant SpoAs. For registration with the SpoA, see procedures as described in clause 6.2.1.

The difference compared to clause 6.2.1 and this scenario is that the service attachment SpoA may involve attachment with SpoA at the home domain or in the visiting domain. Address translation and firewalls may block the terminal from directly accessing the SpoA. It is the responsibility of the registrar to provide the terminal with SpoAs that can be used by the terminal.

6.3.4 De-registration

Procedures same as clause 6.2.4 but with the added complexity that the home servers need to be informed as well. This is shown in the bottom half of figure 11.

7 Simple call applications and services

The following clauses describe how the services described in the [1] can be supported with the meta-protocol. The services being referred to in [1] are:

- Simple call setup
- Simple call setup with ICF,
- Support for Intra-Domain QoS,
- Support for CLIR/CLIP,
- Billing,
- Lawful Interception,
- SCN Interworking,
- VoIP domains Interconnect supporting IP Address Translation,
- VoIP domains Interconnect supporting Interdomain QoS,
- Roaming,
- Number Portability,
- Priority Calls,
- Emergency Calls,
- Carrier Selection.

7.1 Simple call

7.1.1 Initiating the call

This clause gives an example of a simple call as defined in [1]. The basic flows are shown in figure 11.

- The originating Terminal receives a Call set-up indication from its user, the Calling Party. The terminal initiates the Call and Bearer Request to its NWFG (the SpoA). The Identity of the NWFG is provided upon Registration (see clause 6). In TIPHON systems, no direct routed calls between the Calling party and the Called party are allowed. The parties involved in any kind of communications must be authenticated and authorized by the service provider, to use any services.

The Call and Bearer Request includes a variety of information, such as:

- Calling party ID;
- Called Party ID;
- Presentation Restriction Indicator;
- Operator Selection Capability;
- Authorization tickets (for authorized services);
- Send/Receive Media Addresses;
- QoS requirements;
- Codec information, etc.

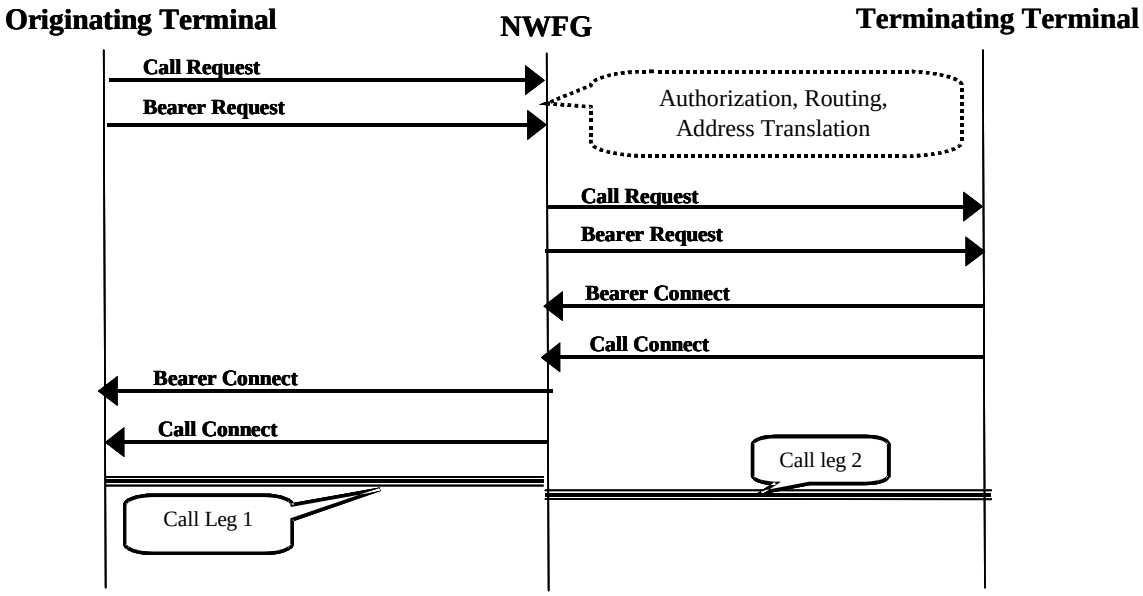


Figure 12: Simple call set-up

- When the Call and Bearer Request arrives at the NWFG, the NWFG performs, amongst other, the following operations:
  - Authorization: Validate the ticket.
  - Accounting: create CDR records for accoutring and billing, etc.
  - Check user/service profile for preferences, special routing issues, etc.
  - Call Routing: an appropriate route/destination is decided to forward the Call and Bearer Request to the next hop.
- The Call Request is forwarded by the NWFG towards the destination (or next hop). Some of the information in the Call and Bearer Request is appended. In the case of CLIR service, the Identity of the Caller may also be hidden from the Called party (this service is discussed later in detail).
- When the Call and Bearer Request arrives at the terminating terminal, several things could happen. The Called user may be busy or on another Call, so the call could either be queued at the terminal or Cleared Down with the "User Busy" Release Reason; the terminal could start to ring, and a "Call Report" "Alerting" could be sent back to the NWFG and the user.
- When the Called party answers the call, the Call and Bearer Connect signal is sent to the NWFG. The "Connect" message includes amongst other information, the media addresses of the Terminating Terminal.
- The Call is now in active phase and media flows.

7.1.2 Clearing the call

- Either party can initiate the "Call Clear-down". Figure 12 shows that the calling party initiates the call clear-down, by sending a "Call Clear request" to the NWFG. The NWFG Sends the "Call Clear Request" to the Called party. The Called party then "hangs- up" and a "Call Clear Confirm" message is sent back to the NWFG.

- The NWFG Sends the "Call Clear Confirm" message to the Calling party, and clears down any resources it had reserved for the call.

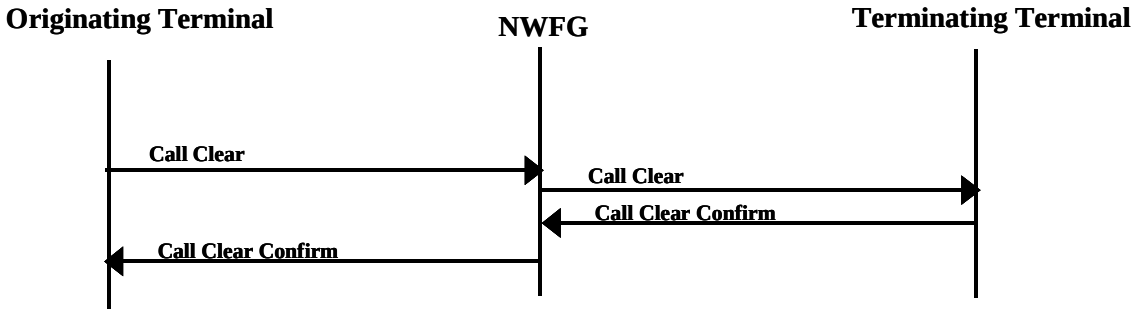


Figure 13: Call Clear-down

7.2 Simple call with ICF

This scenario is an extension of the scenario above. One or more Inter-Connect Functions (ICF) may be along the (media) path of the call, either as explicit middleboxes or embedded in a router/switch. The NWFG instructs the ICFs to let the media pass. The ICF shall inform the NWFG of any address translation the ICF shall employ on the media flow.

The call is initiated in the same way as shown above.

- When the Call and Bearer Request arrives at the NWFG, the NWFG performs the following additional operations:

  - Address Translation and Routing: The destination address analysis takes place here, and.

  - The NWFG also reserves the resources at the ICF by sending it a "Transport Reservation Request". The ICF shall provide the NWFG with any addresses that it might change.

- The Call Request is forwarded by the NWFG towards the destination (or next hop). Some of the information in the Call and Bearer Request is appended, e.g. the Media addresses of the Originating terminal are replaced by the media addresses of the ICF, so that the media would flow from the terminal to the ICF, ICF to destination (or the next hop).

- When the Called party answers the call, the Call and Bearer Connect signal is sent to the NWFG. The "Connect" message includes amongst other information, the media addresses of the Terminating Terminal. The NWFG modifies the Bearers by sending a "Media Establish Request" to the ICF. The NWFG then sends a Call and Bearer Connect message to the Calling party.

Figure 13 shows the amended flows. Note that there is only one ICF shown. In real scenarios one NWFG may communicate with two ICFs, one at each end of the network.

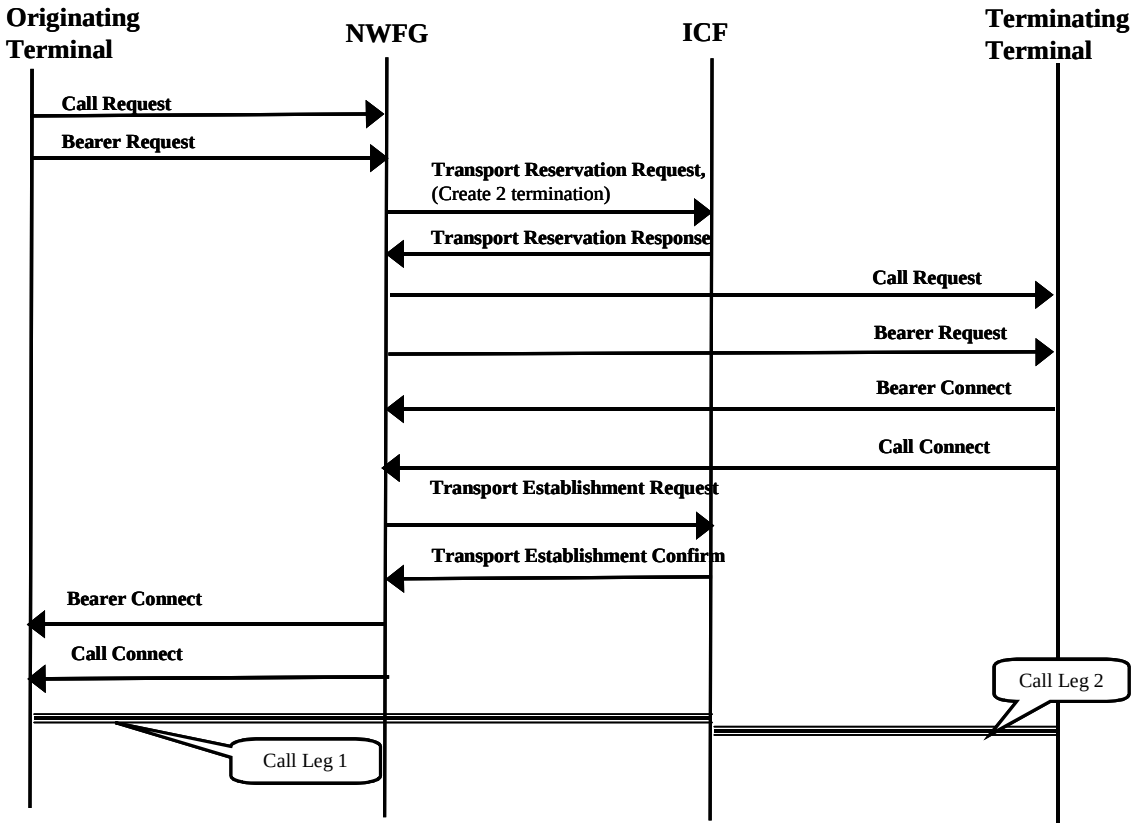


Figure 14: Simple call with ICF

7.3 Support for intra-domain QoS

This clause describes how the meta-protocol can be used to setup a call with a required Quality of Service, within a domain. The difference with the previous clause is that the QoS information is passed in the signalling. This triggers the QoS algorithms to be executed at the NWFGs.

- The Terminal issues a Call and Bearer Request. The Bearer Request includes the Bearer information such as Send/Receive addresses, as well as the required QoS information. The QoS information could include:
  - The Service Class,
  - Codec Descriptor,
  - Delay Budget, etc.
- The NWFG receives the Call and Bearer Request, and requests the ICF to reserve the required resources for the call. This includes creating two Terminations: a Send/Receive Termination towards the Calling Party; and a Send/Receive Termination towards the Called party. The NWFG also reserves resources such as the requested Codec and Bandwidth etc. The QoS budget is verified. If the QoS budget cannot be met the call is rejected.
- If the ICF has sufficient resources available to support the call, it reserves the requested resources, and responds to the NWFG with a Transport Reservation Confirm message. If the ICF cannot support the call, it responds with the Reject message with appropriate Reason.
- Upon successful reservation of resources, the NWFG initiates a Call and Bearer Request towards the Called party. The Bearer Request includes the required bearer capabilities, as requested by the calling party. If the Called party can support the call, it responds with a Connect message. If the Called party cannot support the call, it responds with the appropriate Call decline message.
- Upon receipt of a Call and Bearer connect message, the NWFG informs the ICF to modify the terminations based on the information it received back from the Called Party. This information includes, for example, the Send/Receive address of the Called party.

- The NWFG then sends a Call and Bearer Connect message to the Calling party.

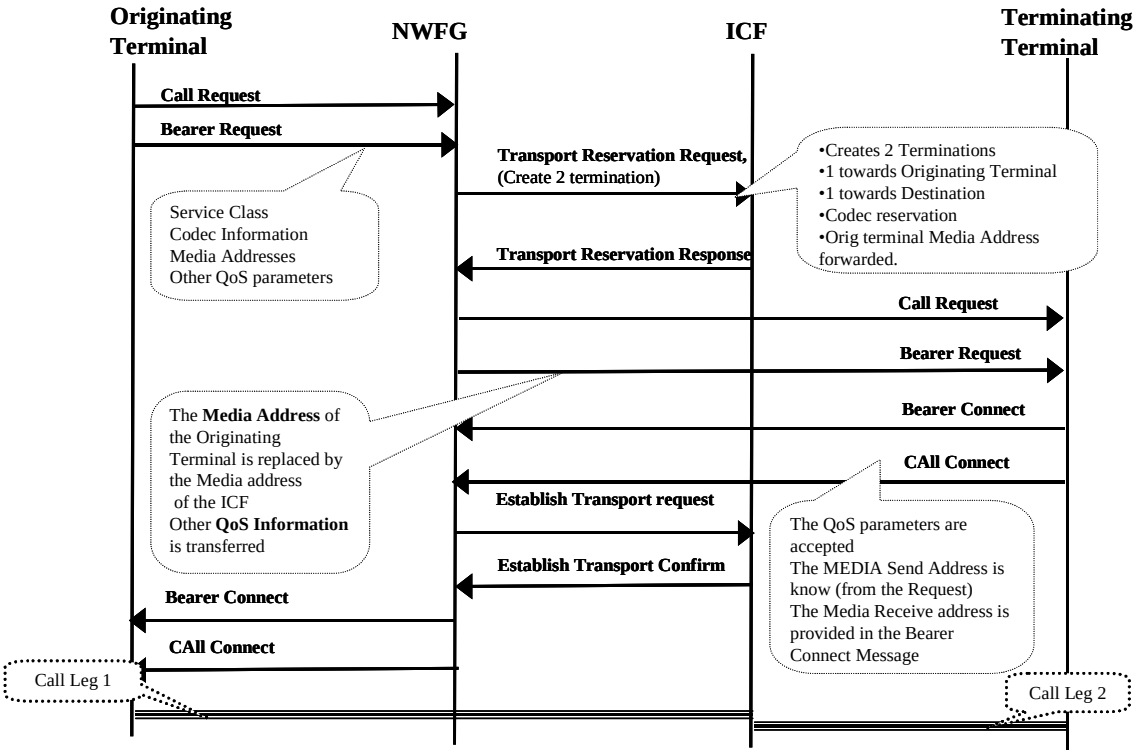


Figure 15: Simple Call with QoS

7.4 CLIP/CLIR

There are capabilities in the meta-protocol to support the CLIP/CLIR service. It can be assumed that the CLIP service will be supported by default. CLIR, however, may require a service invoke request at the terminal or the network. This clause describes how the terminal requested CLIR service can be supported using the meta-protocol.

- When the Caller initiates a call requesting a CLIR service, the "TCC_CallSetup_ind" indicates to the Call Control functionality in the terminal that the user has requested the CLIR service. Therefore, when the Call Control Functionality initiates a Call and Bearer Request, it sets the "Calling Party restriction parameter" to "ID Unavailable"

- The NWFG receives the Call request with the "Calling Party restriction parameter" set to "ID Unavailable". It then initiates a Call Request towards the Called party with the "Calling Party restriction parameter" set to "ID Unavailable".

- When the Called party receives the above Call request, it may accept the "Anonymous" call, or reject it. If the Called party accepts the call, it responds with a Call Connect message.

Note that this is a secure way of providing a CLIR service as the Caller ID or its IP address does not reach the Called party, because the request is proxied by the NWFG. The media flow takes place via the ICF, therefore, the media address of the Calling party is also kept anonymous from the Called party.

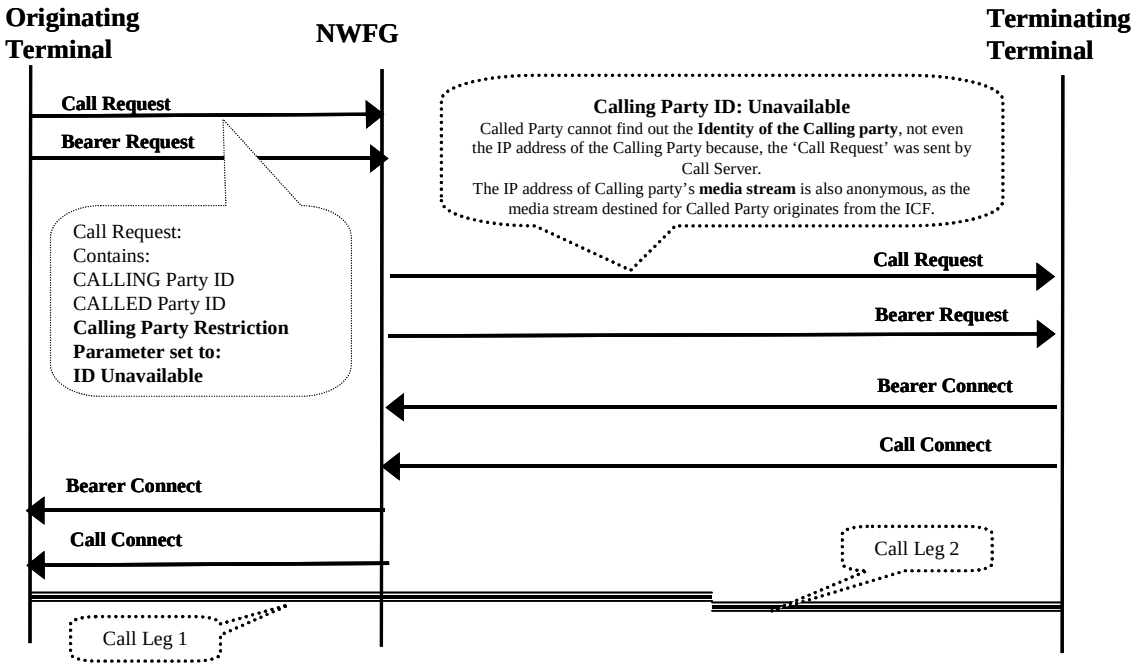


Figure 16: Simple call with CLIP/CLIR

7.5 Event recording

The TIPHON architecture provides support to generate event records, which can be used for various purposes, including Billing. These event records can be generated as a result of Call Control, Bearer Control, and other events, e.g. Call Connect, Bearer Connect. This provides the ability, e.g. to charge, based on either the time duration of a call, or other resource usage, e.g. amount of bandwidth used.

This clause shows the support for accounting information.

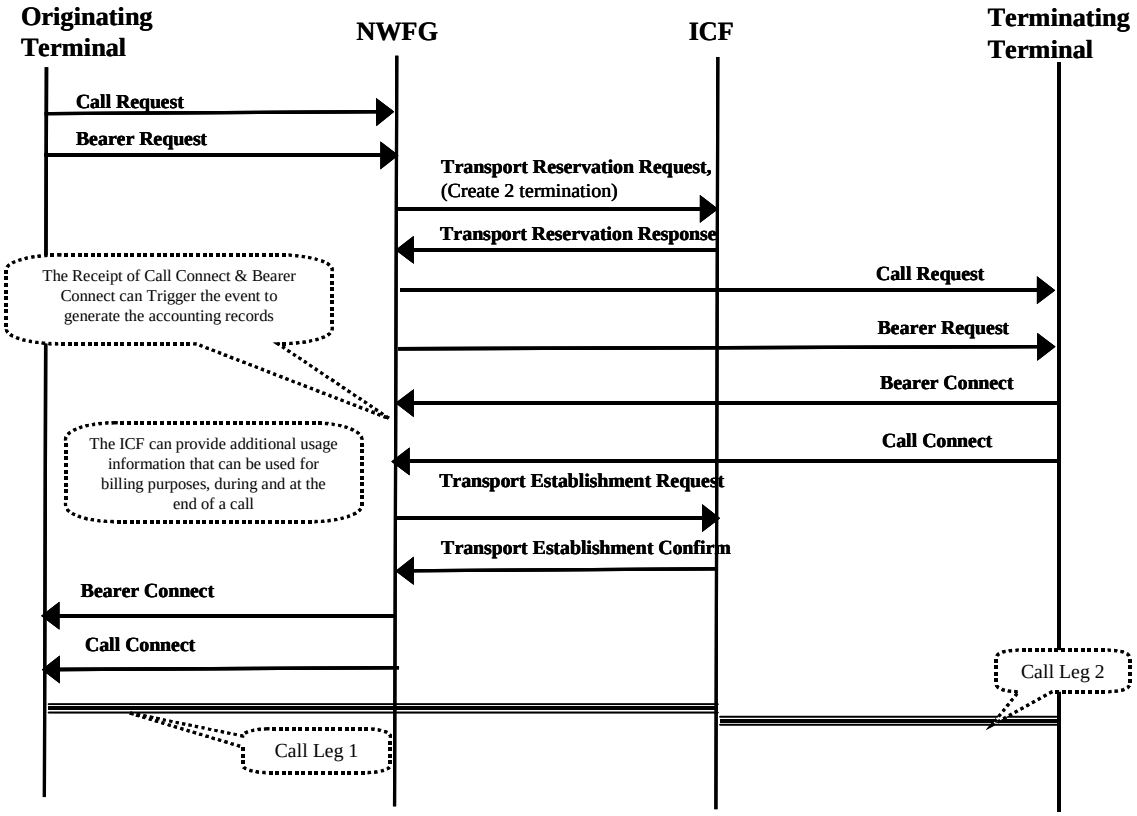


Figure 17: Billing

7.6 Lawful interception

The lawful Interception service is invoked at the NWFG serving the party to be intercepted.

- When a NWFG receives a Call and Bearer Request, it carries out a check to find out if the Subscriber is required to be Intercepted. This could be done via a database query, which is outside the scope of the present document. If the subscriber is not required to be intercepted, the NWFG proceeds with the Call Setup as explained in the clause 7.1. If the subscriber is required to be intercepted, the NWFG sends an "Internal Lawful Interception Data Record" to inform the LI server of the initiated call request.

NOTE: This example of LI deals only with the outgoing call, the procedures for LI at the NWFG may equally apply for an incoming call.

- The LI server may only require the information about outgoing/incoming calls. But, it may also require a copy of the media/data stream between the Calling and Called parties. In such a case, an indication may be sent back to the NWFG to send a copy of the media stream to the LI server.

- If a copy of the media stream is required, the NWFG requests the ICF to create 3 Terminations/flows: one Send/Receive Termination towards the Calling party; second Send/Receive Termination towards the Called Part; and a third Send Termination towards the LI server. The third Termination will send the copied media stream to the LI server.

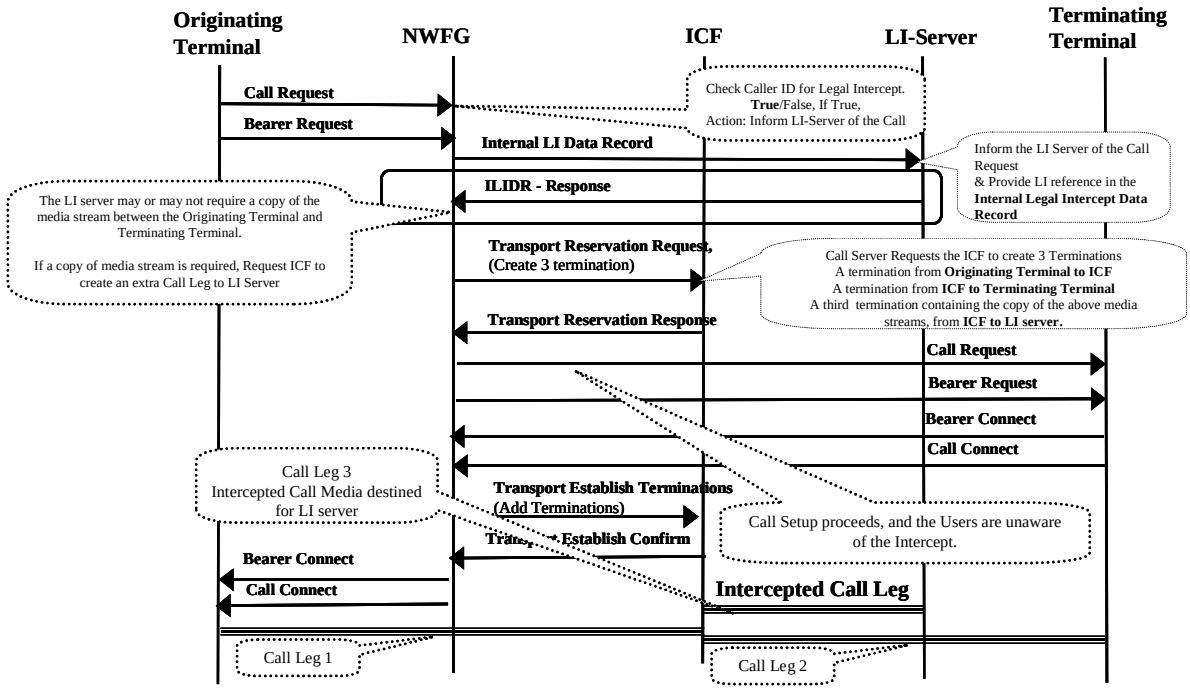


Figure 18: Lawful interception

- The Call setup between the Calling and Called party then proceeds as normal, and both the parties are unaware of the call Interception. When the Called party sends a Call and Bearer Connect message, the NWFG modifies the media information at the ICFs, and an Intercepted Call Leg is activated between the ICF and the LI server.

7.7 IP and SCN interworking

The Signalling Interworking between the VoIP protocols (such as H.323/SIP) and the SCN protocol (such as SS7) takes place at the gateway Functional grouping. The media interworking, i.e. IP to PCM, takes place at the Media Gateways.

The following Call Flows show an overview of simple interworking scenario between a Caller on an IP terminal calling a subscriber on the SCN. These meta-protocol flows are symmetrical, so they apply equally to the scenario of SCN to IP Call setup.

- The caller initiates the call at the Originating terminal, and a Call and Bearer Request is sent to the NWFG.
- The NWFG carries out any address translation, performs routing checks, and routes the call to the SCN Gateway. The SCN gateway also acts as a NWFG, and routes the call request to the SCN.
- The bearer from/to the terminal is tied to the ICF: this is Call Leg 1. The second Call leg is between the ICF and the Media Gateway, and the Third Call leg is between the Media gateway and the SCN.

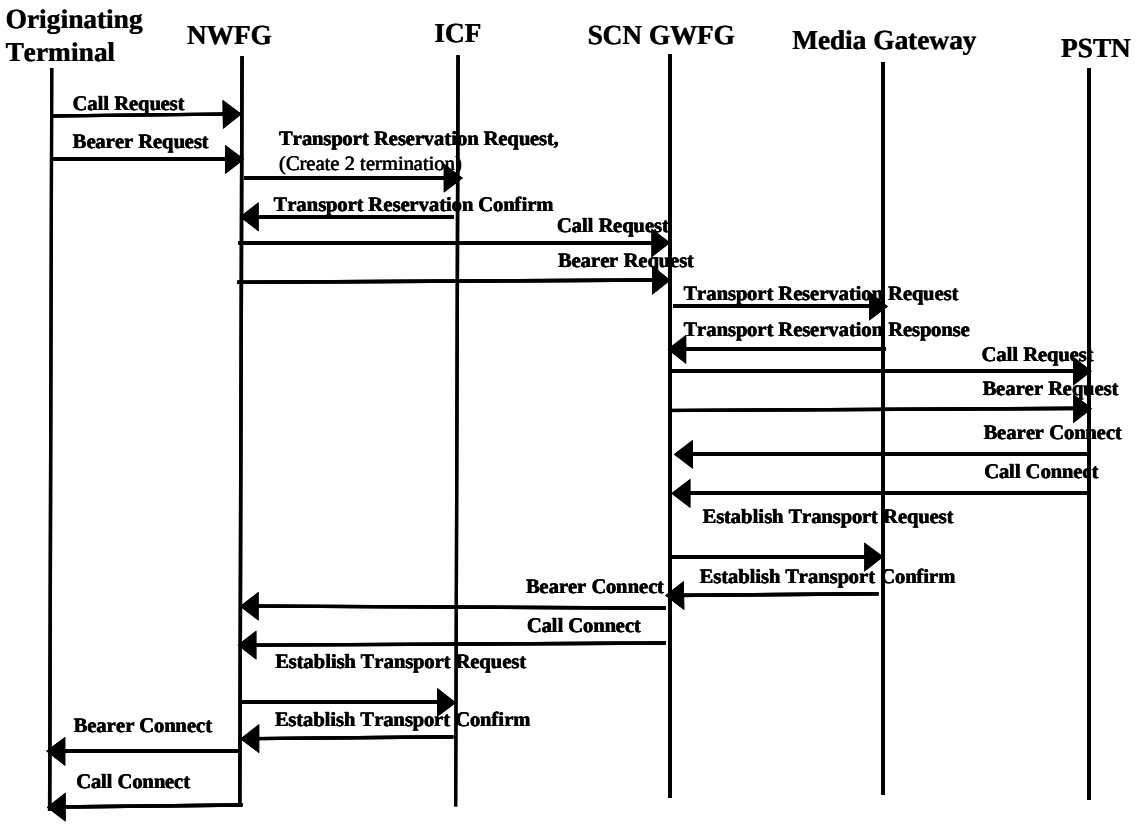


Figure 19: IP to SCN interworking

7.8 VoIP interconnect

The VoIP Interconnect refers to a service where two or more VoIP domains provide VoIP service to each other. There would be SLAs between the interconnecting domains governing the flow of traffic between the domains, support roaming subscribers, and possibly provide service ubiquity.

TS 101 878 [1] identifies three types of interconnects:

- Service level interconnection

Meta-protocol can provide the support for the service level interconnection, provided the interconnecting domain supports the service capabilities, as supported in the home domain.

- Roaming level interconnection

Meta-protocol can provide support for the roaming level interconnection. The signalling is relayed to home domain, and the call processing, where the call processing and service execution takes place.

- Transport level interconnection.

Meta-protocol currently supports IP as the transport layer.

Some of the main issues when providing an interconnect are:

- Address translation. A VoIP domain may use a private addressing scheme, NAT, which may hamper the media path setup in between the two domains.

- Support for QoS. This could be SLA based.

- Charging, whether usage based or session duration based, needs a mechanism to support both; TIPHON supports them both.

7.8.1 VoIP interconnect with an example of IP address translation

This clause shows how a VoIP Interconnect takes place between two domains, with the support of the meta-protocol. See figure 20. This example highlights the VoIP interconnect with address translation.

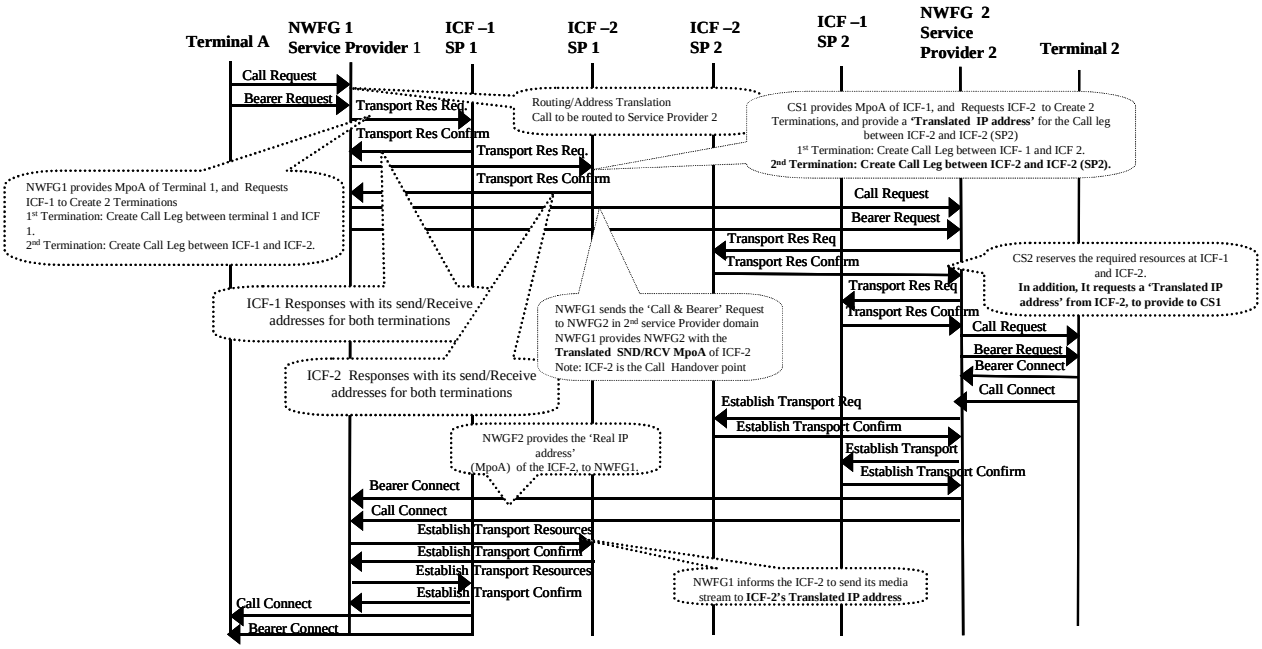


Figure 20: VoIP Interconnect with an example of address translation

- When the NWFG 1 receives a Call and Bearer Request, it carries out address translation/Routing checks. It finds out that the called party is subscribed to another domain, and finds the interconnect ICF between domain 1 and 2.

NOTE: It is assumed that both the domains 1 and 2 use a private addressing scheme.

- NWFG 1 reserves resources at the ICF-1 (SP1), and ties the Calling party Bearer to one of its Terminations. NWFG 1 then reserves resources at the ICF-2 (SP1), and ties one of its Terminations/flow descriptors to the second Termination of ICF-1 (SP1).

- NWFG 1 also requests the ICF-2 (SP1) to provide a "Translated IP address" for the Termination/flow descriptor towards the InterConnect Function, ICF-2 (SP2), of the second domain.

- The Translated IP address is then transported in the Bearer Request to the NWFG-2 (SP2). This is to make sure that the NWFG 2 (SP2) sends the media stream to a **reachable address**, and not a private address behind NAT.

- The NWFG 2 (SP2), upon receipt of Call and Bearer Request reserves the resources at ICF-1 (SP2) and ICF-2 (SP2), and ties the relevant bearers.

- The NWFG-2 also requests the ICF-2 (SP2) to provide a "Translated IP address" for the Send/Receive Termination flow descriptor towards the ICF-2 (SP1). This is to make sure that the media stream from the originating Domain is sent to a reachable address.

- Upon successful call setup, the NWFG-2 modifies the relevant resources, and sends a Connect message back to the NWFG-1, along with the "Translated" media address of the ICF-2 (SP2).

- The NWFG-1 modifies the relevant resources, and sends a Connect message back to the originating terminal.

- The media in the Originating Domain flows between the originating terminal and the ICF-2, and the media in the Terminating Domain flows between the ICF-2 and terminating terminal. The media between the two domains flows between the two ICF-2s.

7.8.2 VoIP interconnect with an example of QoS

This clause highlights the support for QoS for calls originating from one domain, and terminating in another domain. See figure 21. This clause provides the QoS support for inter-domain calls.

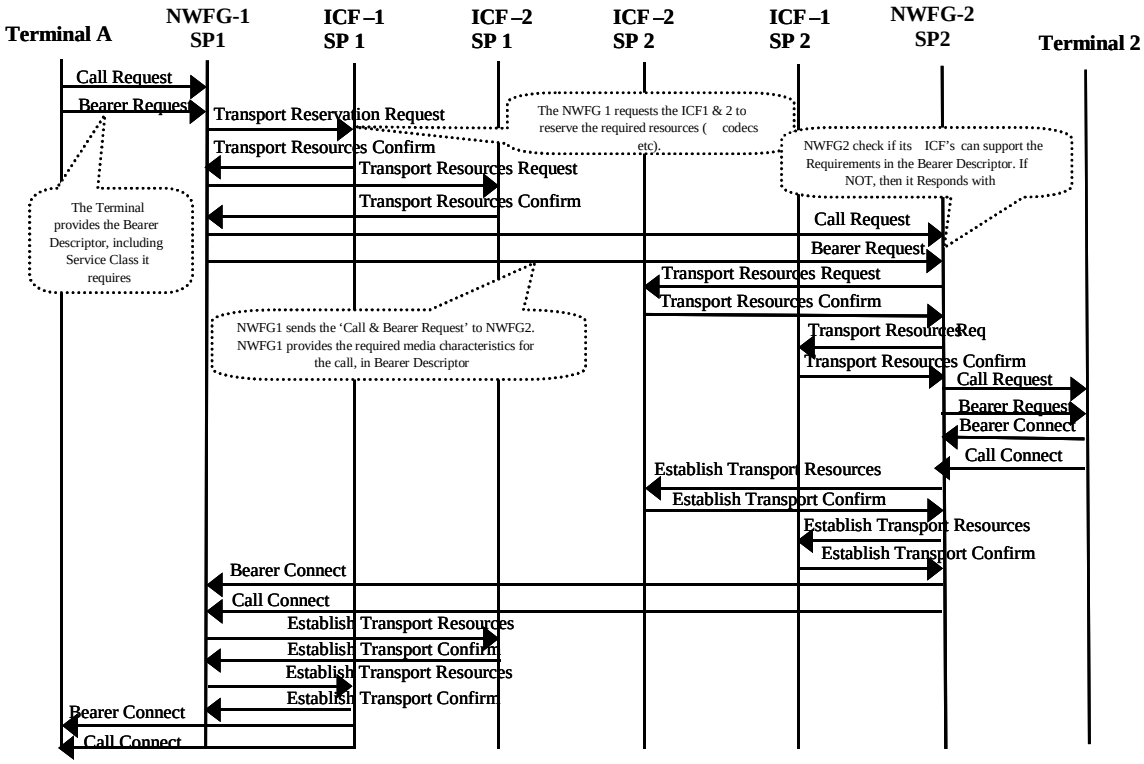


Figure 21: VoIP interconnect with an example of QoS

- The terminal provides the Bearer Descriptor in the Bearer Request.
- The NWFG-1 requests ICF-1 and ICF-2 in the originating domain to reserve the required media resources.
- Upon successful media reservation, the NWFG-1 sends a Call and Bearer Request to the C NWFG-2, in the terminating domain. The Bearer request includes the required QoS for the call.
- The NWFG-2 checks if it (its domain) can support the required QoS level. If it can, it reserves the media resources at the relevant ICFs, and continues with the call setup. If the NWFG-2 cannot support the QoS level, it will reject the call providing the relevant reason.

7.9 Roaming User scenario

This clause shows how the home services are provided to a roaming subscriber in a visiting domain. It is assumed that there exists at least a "Roaming level interconnection", and a "Transport level interconnection" between the home and visited domain. Also, the roaming subscriber is authorized for the roaming service, and that it has successfully registered (see clause Registration). Figure 22 shows a scenario where the Call signalling and the Bearer flow to/through the home network. There could also be a scenario, as shown by figure 23, where only the Call Signalling goes to the home domain for call processing/service execution, and the bearer flows directly between the originating and terminating domain, bypassing the home domain. This may be done for an efficient usage of resources.

- The roaming subscriber issues a Call and Bearer Request to the NWFG in the serving domain (SD). The NWFG in the Serving domain is identified as per clause: Registration. The NWFG has been notified of the roaming user and the call treatment for the roaming subscriber, during registration. The NWFG (SD) checks the home domain ID in the call request, realizes that the Call is from a roaming subscriber, who is authorized to make this call. The NWFG reserves the necessary resources in its domain (at the ICF) to:
  - support the required QoS level,
  - tie the bearers in both directions.
- The NWFG then sends a Call and Bearer Request to the Home Domain of the Caller.
- The NWFG in the Home Domain validates the Call Request, performs any service execution, reserves the required resources, and sends a Call and Bearer Request to the called party.
- The called party could be in the Home domain, in which case the Bearer will be set-up between the visiting domain and the home domain, as shown in figure 22. It may, however, be the case where the terminating domain is not the Home Domain. In such a case, the Bearer may still be setup through the home domain, or it may be setup directly between the serving and terminating domain, for an efficient usage of resources, as shown in figure 23.

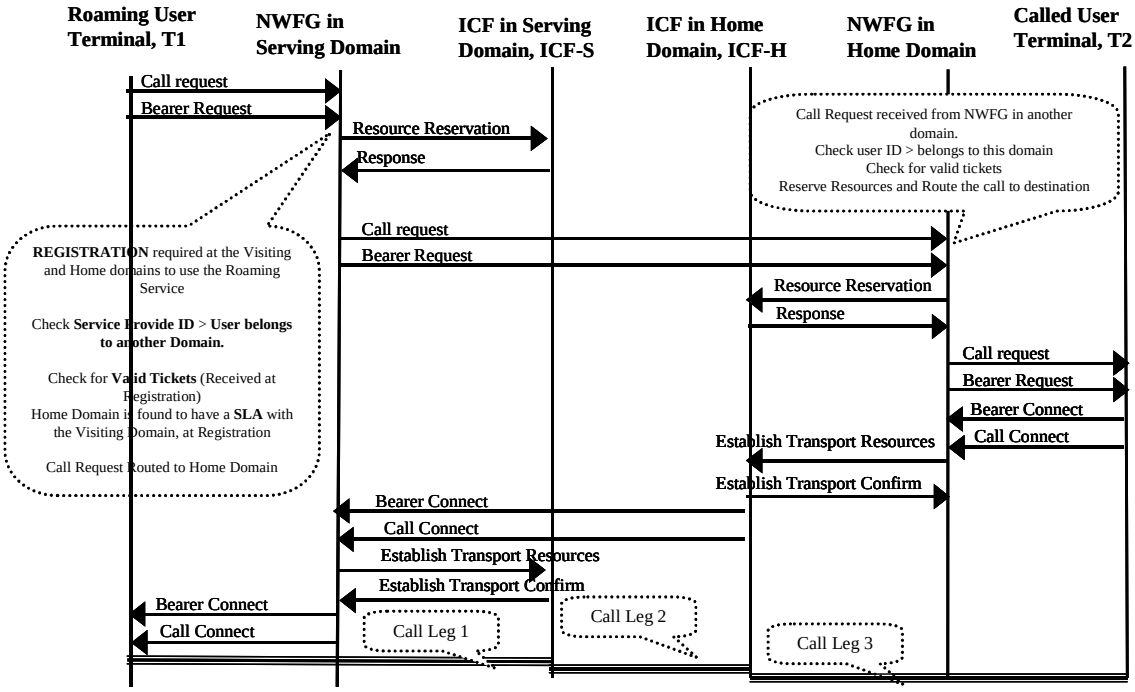


Figure 22: Call set-up for roaming user - Call and Bearer via home domain

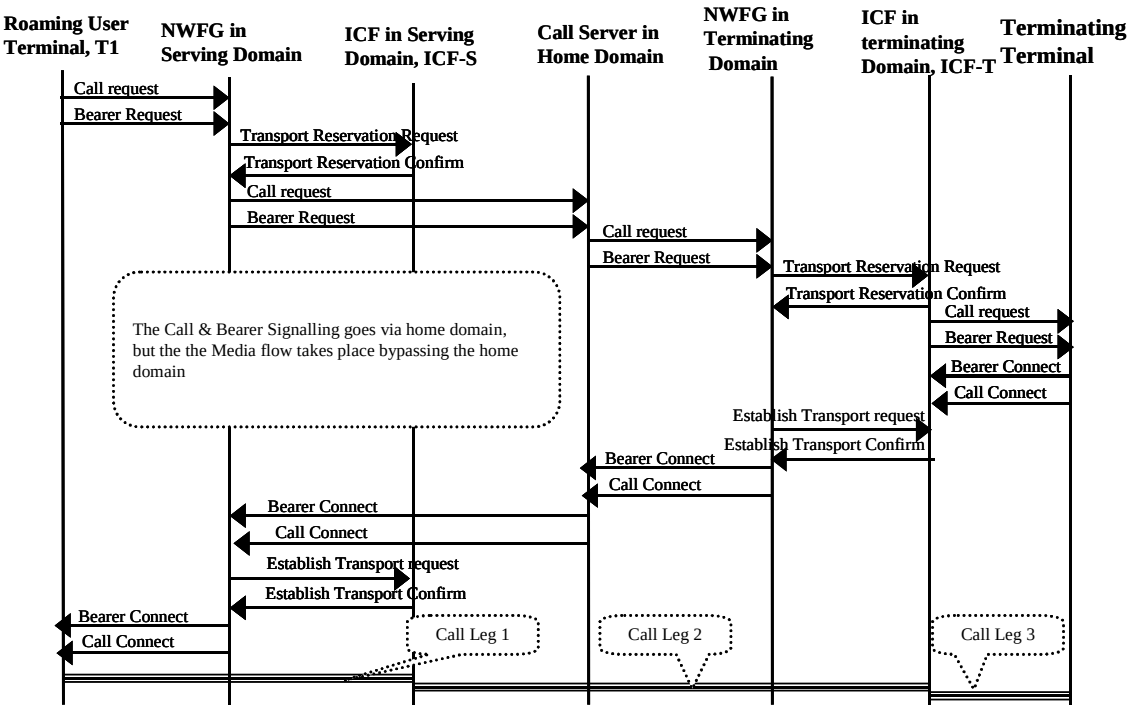


Figure 23: Call set-up for Roaming user - Only call control signalling via home domain

7.10 Number portability

TS 101 878 [1] describes the support for three flavours of number portability:

- All Call Query (ACQ).
- Pivot Routing.
- Query on Release (QoR).

This clause describes the support provided by the meta-protocol to support Number Portability including all the three flavours above.

7.10.1 Number portability - All Call Query

The procedure to support ACQ is described below.

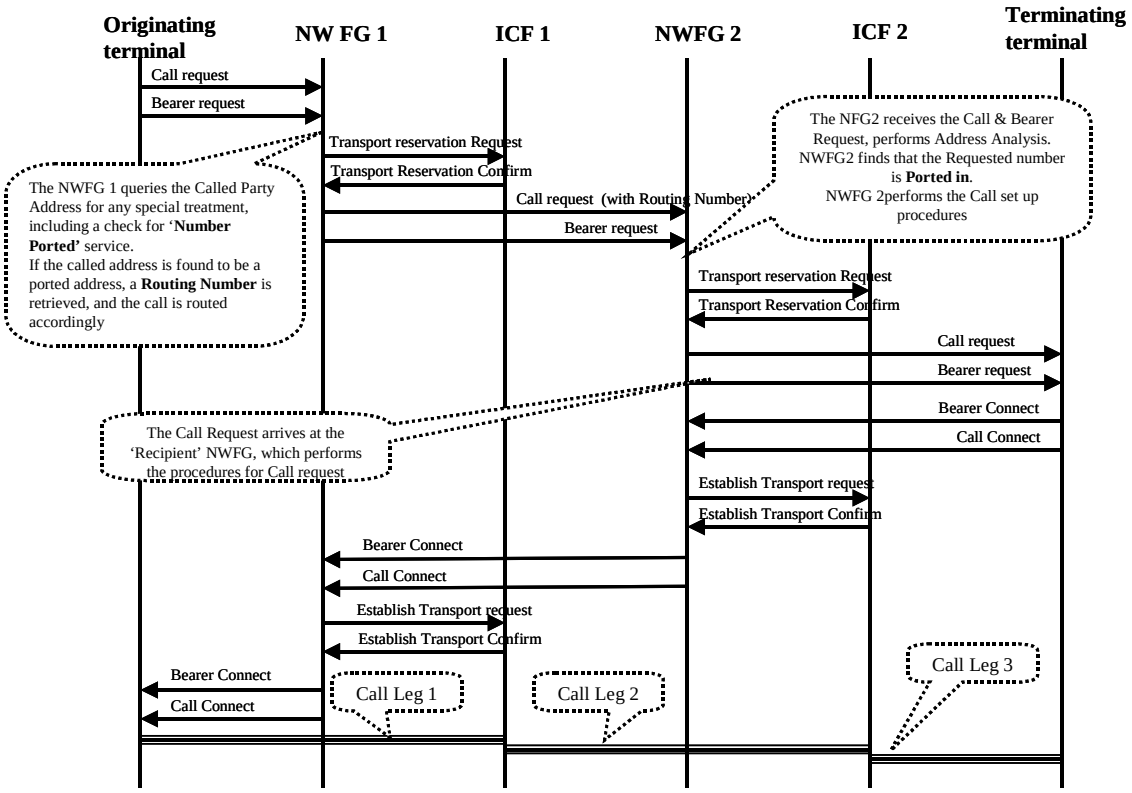


Figure 24: Number Portability - All Call Query

- When the Call and Bearer Request is received by the NWFG, it performs a Called Address Analysis, which includes a check for Number portability. The specific method used for the Number Portability check is outside the scope of the present document.
- If the Number portability check returns a value confirming that the called address is a ported address, a "Network Routing Number" is obtained.
- The Call and Bearer setup is then carried out as per clause 7.1, with one exception: The Call is routed to the Recipient NWFG, based on the Network Routing Number, which is included in the Network_Call_Setup message of the meta-protocol.

7.10.2 Pivot routing

7.10.2.1 Call drop-back

- The Originating NWFG receives a Call and Bearer Request, and performs routing query. The Call and Bearer Request is sent to the NWFG 2.
- The NWFG-2 receives the call request for the Called subscriber, performs a location query, and finds it to be "ported-out". The NWFG-2 responds to NWFG-1 with a Call Report. The "Report Reason" parameter is set to "User Moved". The Call Report also includes the "Report Parameter", providing the "Network Routing Number".
- The NWFG-1 re-initiates the call setup, based on the routing information it received from the NWFG-2. The routing may be direct to the recipient network (shown), or indirect (not shown).
- The Call Request arrives at the Recipient NWFG (NWFG-3). The NWFG-3 performs the address analysis and finds the called subscriber to be "ported in". The Called subscriber is located and the call set-up proceeds as defined in clause 7.2.

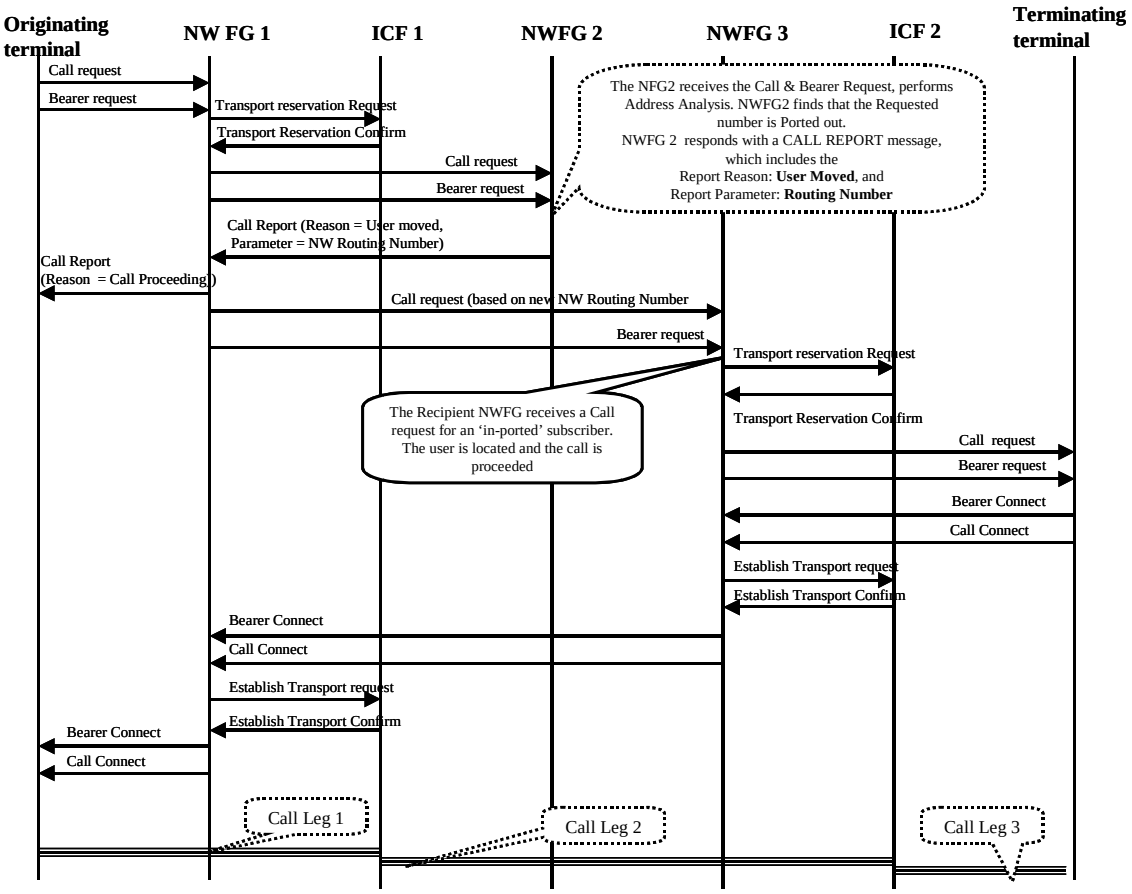


Figure 25: Number portability - Call drop-back option

7.10.2.2 Onward routing

- The Call and Bearer Request arrives at the NWFG-1. NWFG-2 is found to be the destination NWFG, and the Call and Bearer Request is routed to NWFG-2.
- The NWFG-2 performs the address analysis, finds the Called party to be ported out.
- The NWFG-2 determines the new address/route to the Called party, and the call is routed to the "Recipient" NWFG.
- The rest of the procedures are same as previous clause.

The following call flows show the meta-protocol support for Pivot routing.

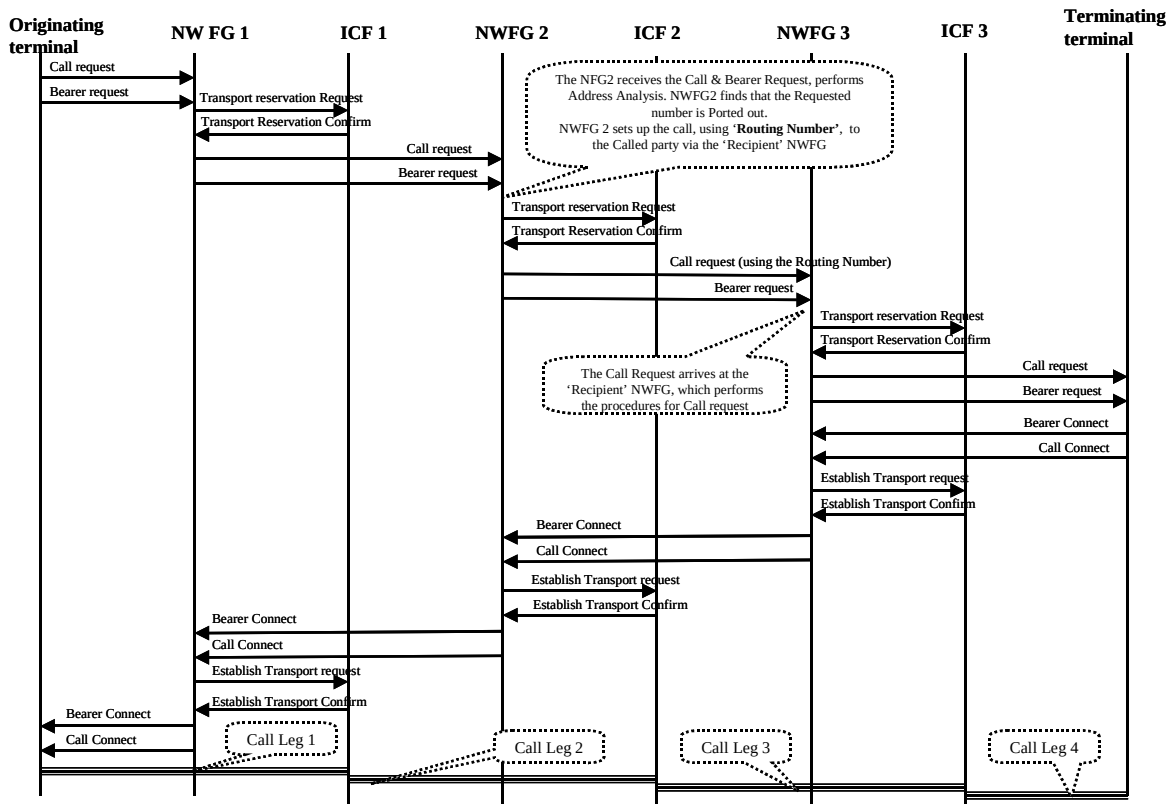


Figure 26: Number portability - Pivot routing

7.10.3 Query on Release (QoR)

This clause describes the support for QoR method to support number portability.

- The first part of the call setup is performed as described in clause 7.2. The Call and Bearer Request arrives at the serving NWFG, which performs the routing function, and the Called party is found to be served by the NWFG-2.
- The Call and Bearer Request is routed to the NWFG-2.
- When the Call and Bearer Request is received at the NWFG-2, the Called party is found to be ported out.
- The Call and Bearer Request is rejected. The meta-protocol Reject message includes the reject reason: "Moved".
- The NWFG-1 receives the Reject message, checks the reject reason, and queries (possibly a database) for the routing number to destination.
- The routing number is provided to the NWFG-1, by means outside the scope of the present document.
- The NWFG-1 routes the call request to the Recipient NWFG-3, based on the routing number it received.
- The rest of the call set-up takes place as per clause 7.2.

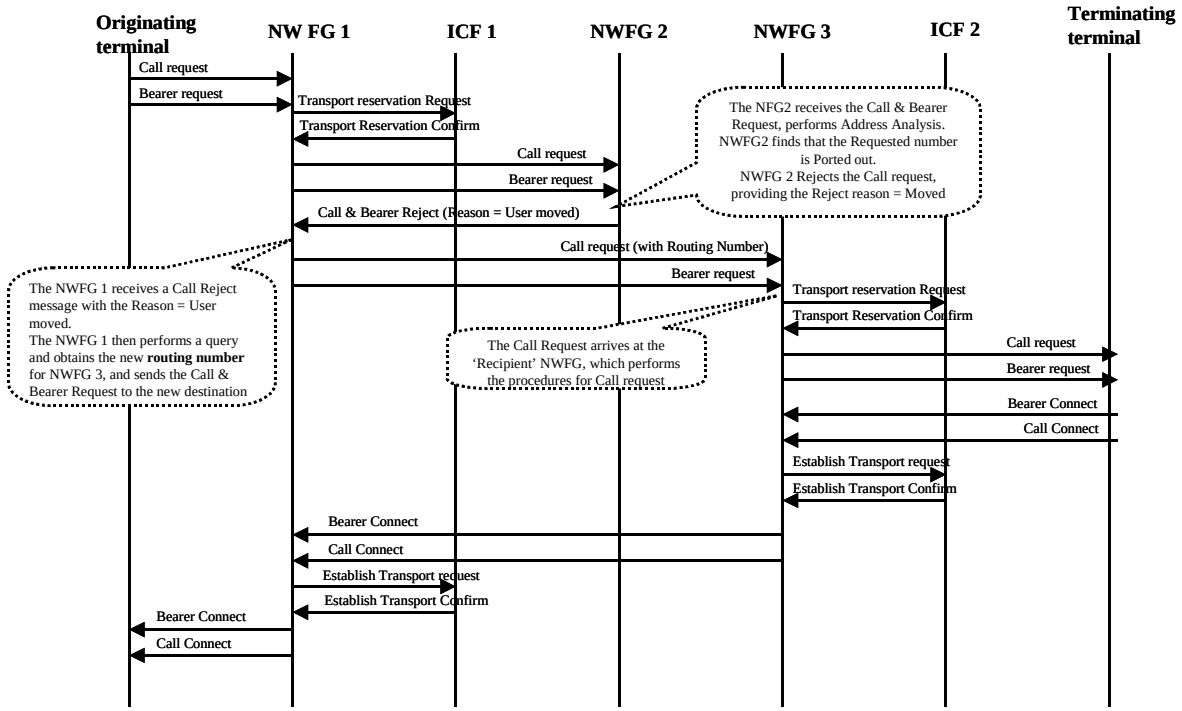


Figure 27: Number Portability - Query on Release

7.11 Priority Calls

The Authorized Priority Call Service (APCS) enables specific users to make priority calls to any destination from any served point. The TIPHON meta-protocol has the capabilities to support the Authorized Priority Call Service. The "Priority" parameter in the Call request can be set to treat the calls, in the network, according to their priority levels. It is assumed that the user is able to access the network through some access medium (outside the scope of the present document), and the network provides the priority treatment to complete the call. The network can be notified of the priority of the call in several ways.

- Terminal/User selected.

  When a terminal/user sends a Call request, the call priority can be set as required, e.g. in a similar way as email. The network may however, ignore this or require user authorization to utilize the service.

- Service Code.

  Upon registration, the user requests, and if authorized, is provided with a priority call service. When the user requires a priority treatment for a call, he indicates this in the Call request message. The priority level can also be pre-set in the network based on the user ID (activated upon registration).

The user may also be provided with a service code to access the APCS service. The user then provides the service code to use the priority call service, each time it requires the service.

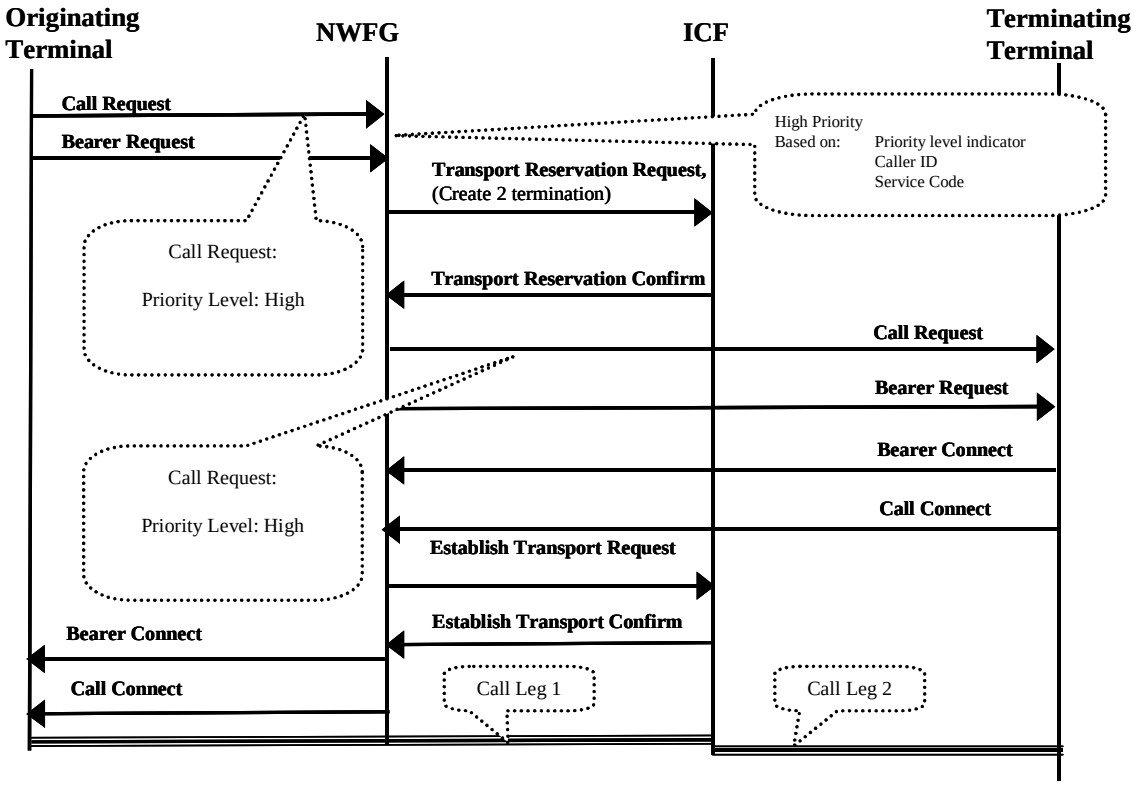


Figure 28: Priority Calls

- When the user requires a priority treatment to a call, he either indicates it to the NWFG in the Call Request (Service Offer ticket = priority call), or provides the service code to gain priority treatment. The authorization process for this purpose is outside the scope of the present document.

- The NWFG receives a Priority indication in the Call request message, and reserves network resources to provide a priority treatment to the call.

- The NWFG then sends a Call and Bearer Request to the Called party or other nodes in the network. As this call request for a priority call is generated by a NWFG, the other nodes in the path provide the required service without authorizing the Caller.

7.12 Emergency Calls

Emergency Call is similar to the Priority call. The emergency call is usually invoked by a Service Code associated with the emergency services, e.g. 112, 911, 999, or a URL. The terminal/user can set the priority field, but it is the NWFG that is responsible to provide the necessary resources, carry out the necessary address translation, and route the call to the emergency services call centre. The following example shows how the meta-protocol provides the support for emergency services.

- The Caller issues a Call and Bearer Request, by providing the emergency services code.
- The call request is received by the NWFG, which carries out the address translation and routing. Bearer set-up is also carried out at this stage.
- The Emergency Call Request is sent to the Emergency Call centre, and the call is connected to an operator. The treatment of the emergency from Emergency Call centre onwards is outside the scope of the present document.

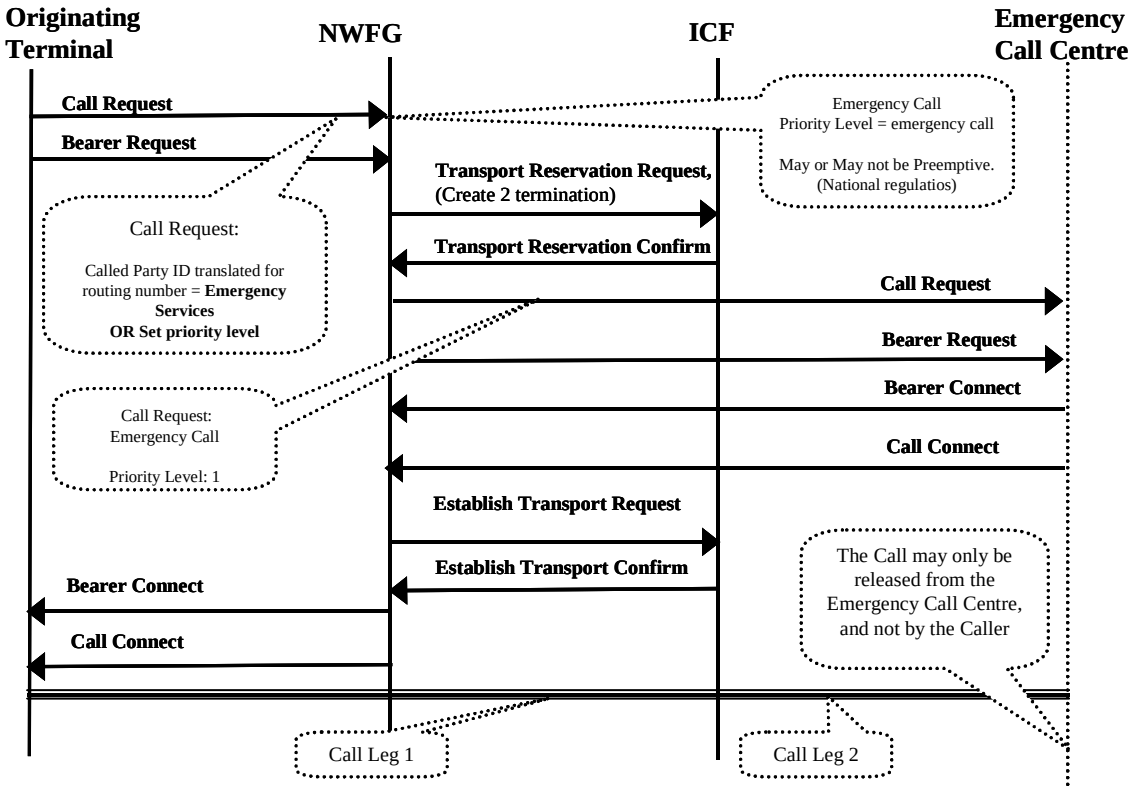


Figure 29: Emergency Call

7.13 Carrier Selection

Carrier selection service can be invoked on a per call basis, or pre-selected for all calls.

In the case of per call carrier selection, the Caller may provide the "Carrier Code" in the "Operator Selection" parameter in the meta-protocol, or simply dial the service code prefixed to the Called number. In either case, the NWFG performs the address and service translation, and routes the call to the required carrier.

In the case of Carrier pre-selection, all calls are routed to the requested carrier.

Figure 30 shows how the meta-protocol supports the carrier selection on a per call basis:

- The Caller initiates a Call and Bearer Request, and provides the service code for the selected carrier.
- The NWFG receives the Call request and reserves the required resources. A Call leg is initiated between the Calling party and the ICF in the originating domain.
- The Call Request is then sent to the NWFG in the selected carrier/domain. The NWFG in the Selected Carrier/domain then performs the call processing/routing etc. as well as reserve resources for the call.
- When the NWFG in the Selected domain receives a Call and Bearer Connect message, it sends a Call and Bearer Connect message to the NWFG in the Originating domain. The Media Resources are modified at the ICFs, and the Calling party is connected to the Called party.

Note that the address translation and QoS procedures as defined in the IP Interconnect section still apply.

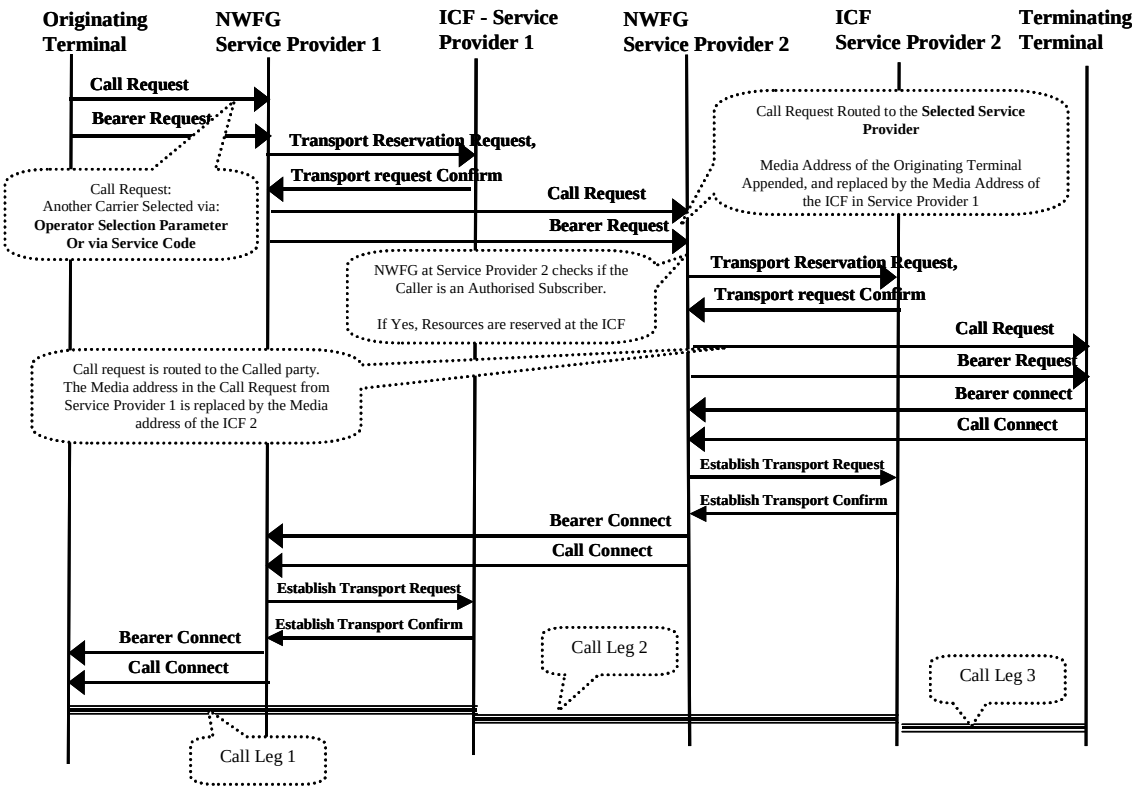


Figure 30: Carrier Selection

Annex A (informative): Bibliography

ETSI TS 101 884: "Telecommunications and Internet protocol Harmonization Over Networks (TIPHON) Release 3; Technology Mapping; Implementation of TIPHON architecture using SIP".

ETSI TS 101 332: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Interface Protocol Requirements Definition; TIPHON Extended MEGACO Package (EMP) Specification".

DTS/TIPHON-03028R4: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Interface Protocol Requirements Definition; Technology mapping of TIPHON architecture to Extended MEGACO Package".

List of figures

Figure 1: Relationship with other TIPHON Release 3 documents 6
Figure 2: Meta-protocol enabled interworking 11
Figure 3: TIPHON application architecture 12
Figure 4: Example implementation of TIPHON architecture 13
Figure 5: Call set-up using meta-protocol 14
Figure 6: General structure of the TIPHON registration mechanism 15
Figure 7: Service attachment 16
Figure 8: De-attachment 16
Figure 9: Simple user registration 17
Figure 10: Roaming architecture 19
Figure 11: Full roaming sign-on scenario 19
Figure 12: Simple call set-up 22
Figure 13: Call Clear-down 23
Figure 14: Simple call with ICF 24
Figure 15: Simple Call with QoS 25
Figure 16: Simple call with CLIP/CLIR 26
Figure 17: Billing 27
Figure 18: Lawful interception 28
Figure 19: IP to SCN interworking 29
Figure 20: VoIP Interconnect with an example of address translation 30
Figure 21: VoIP interconnect with an example of QoS 31
Figure 22: Call set-up for roaming user - Call and Bearer via home domain 32
Figure 23: Call set-up for Roaming user - Only call control signalling via home domain 33
Figure 24: Number Portability - All Call Query 34
Figure 25: Number portability - Call drop-back option 35
Figure 26: Number portability - Pivot routing 36
Figure 27: Number Portability - Query on Release 37
Figure 28: Priority Calls 38
Figure 29: Emergency Call 39
Figure 30: Carrier Selection 40

History

Document history		
V1.1.1	March 2002	Publication