UNIVERSITY OF TWENTE.

Master of Science Thesis
University of Twente
Faculty of Electrical Engineering, Mathematics and
Computer Science (EEMCS)
Design and Analysis of Communication Systems (DACS)

Architecture for IP based interconnection of heterogeneous wireless communication systems for mission-critical group oriented communications

Yi Lin
November 24, 2010

Supervisors:
Dr.ir. Georgios Karagiannis (First Supervisor)
Dr.ir. Geert Heijenk
Prof.dr. Hans van den Berg

Abstract

Public safety involves the prevention or protection from emergence events that could cause danger, injury and damage to the general public. Public safety is considered as the largest Professional Mobile Radio market that is served by Terrestrial Trunked Radio (TETRA). TETRA specifies some mission-critical services that can be used in public safety communication system. Currently, three main network scenarios are identified to support these mission-critical services. These three network scenarios are tactical patch, expanding coverage and migration to other network. Within the mission-critical network, interconnection of different users in these three main network scenarios becomes an interesting issue. MPLS (Multi Protocol Label Switching) based IP networking solutions could be utilized to satisfy the requirements imposed by mission-critical services. Therefore the main goal of this thesis project is to specify, design and evaluate an architecture for the interconnection of heterogeneous communication systems using MPLS based IP networks for mission-critical group oriented communications.

In this research, a core network architecture has been designed. To show how the core network architecture can support group communication, we defined message sequence charts for the main features that are supported by the core network. We evaluated the core network architecture with respect to the scalability. Scalability is measured by calculating the number of signaling messages (i.e., signaling load) per selected feature when the number of wireless access networks supported by the core network is increased. Based on the calculation, some graphs associated with the selected features are generated to indicate the performance behavior of various signaling messages for the main features.

Abbreviations

TETRA	Terrestrial Trunked Radio
MPLS	Multi Protocol Label Switching
ETSI	European Telecommunications Standards Institute
PMR	Professional Mobile Radio
DGNA	Dynamic Group Number Assignment
ODINI	On-Demand-Intelligent Network Interface
UMTS	Universal Mobile Telecommunication System
WiMax	Worldwide Interoperability for Microwave Access
LTE	Long Term Evolution
QoS	Quality of Service
SDS	Short Data Service
TDMA	Time Division Multiple Access
SS-PPC	Supplementary Service Pre-emptive Priority Call
CRV	Call Retention Value
SwMI	Switching and Management Infrastructure
SS-CRT	Supplementary Service Call Retention
ITSI	Individual TETRA subscriber Identity
GTSI	Group TETRA Subscriber Identity
SS-AL	Supplementary Service Ambience Listening
MS	Mobile Station
SS-CAD	Supplementary Service Call Authorized by Dispatcher
SS-AS	Supplementary Service Area Selection
SS-LE	Supplementary Service Late Entry
ISI	Intersystem Interface
MCC	Mobile Country Code
MNC	Mobile Network Code
GSM	Global System for Mobile communication
RSVP	Resource Reservation Protocol
IntServ	Integrated Services
IGMP	Internet Group Management Protocol
PIM-SM	Protocol Independent Multicast-Sparse Mode
IPSec	IP Security Architecture
GPRS	General Packet Radio Service
ANF-ISIIC	Additional Network Feature-Inter-System Interface Individual Call
ANF-ISIGC	Additional Network Feature-Inter-System Interface Group call
CSwMI	Controlling Switching and Management Infrastructure
OSwMI	Originating Switching and Management Infrastructure
PSwMI	Participating Switching and Management Infrastructure
ANF-ISIMM	Additional Network Feature-Inter-System Interface Mobility Management
LSP	Label Switched Path
LER	Label Edge Router
LSR	Label Switching Router
FEC	Forwarding Equivalence Class
GMPLS	Generalized Multiprotocol Label Switching
NHLFE	Next Hop Label Forwarding Entry
Diffserv	Differentiated Services

DSCP	DiffServ codepoints
DPS	Dynamic Packet State
NSIS	Next Steps in Signaling
NTLP	NSIS Transport Layer Protocol
GIST	General Internet Signalling Transport
NSLP	NSIS Signaling Layer Protocol
MLD	Multicast Listener Discovery
DVMRP	Distance Vector Multicast Routing Protocol
MOSPF	Multicast Open Shortest Path First
PIM-DM	Protocol Independent Multicast-Dense Mode
CoA	Care-of address
FA	Foreign Agent
LMA	Local Mobility Anchor
MAG	Mobile Access Gateway
HA	Home Address
PBU	Proxy Binding Update
PBA	Proxy Binding Acknowledgement
PMAG	Previous MAG
NMAG	New MAG
PBR	Proxy Binding Registration
NEMO	Network Mobility
MR	Mobile Router
MN	Mobile Node
SNDCP	Sub-Network Dependent Control Protocol
SONET	Synchronous Optical Networking
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
PMIP	Proxy Mobile IP
PTT	Push to Talk

Preface

This thesis is the result of my M.Sc project that is done at the chair for Design and Analysis of Communication Systems (DACS), Faculty of Electrical Engineering, Mathematics and Computer Science (EEMCS), at the University of Twente, The Netherlands.

Regarding my thesis project, I would like to thank my first supervisor Dr.ir. Georgios Karagiannis, who spent many hours on supervising me to finish my M.Sc project. Furthermore, I would like to thank Dr.ir. Geert Heijenk and Prof.dr. Hans van den Berg for their valuable inputs and comments.

Finally, I would like to thank my parents for their understanding and support. Without their love, this thesis could not be accomplished.

Table of Contents

Chapter 1 Introduction

1.1 Background

Public safety is aimed at providing prevention or protection for general public in order to avoid damage and danger. Examples of public safety services are police force, fire brigades, ambulance service, transport police, maritime and coastguard services.

TETRA (Terrestrial Trunked Radio) is a standard proposed by ETSI (European Telecommunications Standards Institute) [ETSI-TETRA] that has been deployed around the globe to fulfill the PMR (Professional Mobile Radio) markets. A good overview of the status of the TETRA system is provided in [TETRA-A]. Typical PMR market segments are public safety, see Figure 1, transportation, utilities, government, military, public access mobile radio, oil and industry. Among all of them, public safety is the largest market that is being served by TETRA.

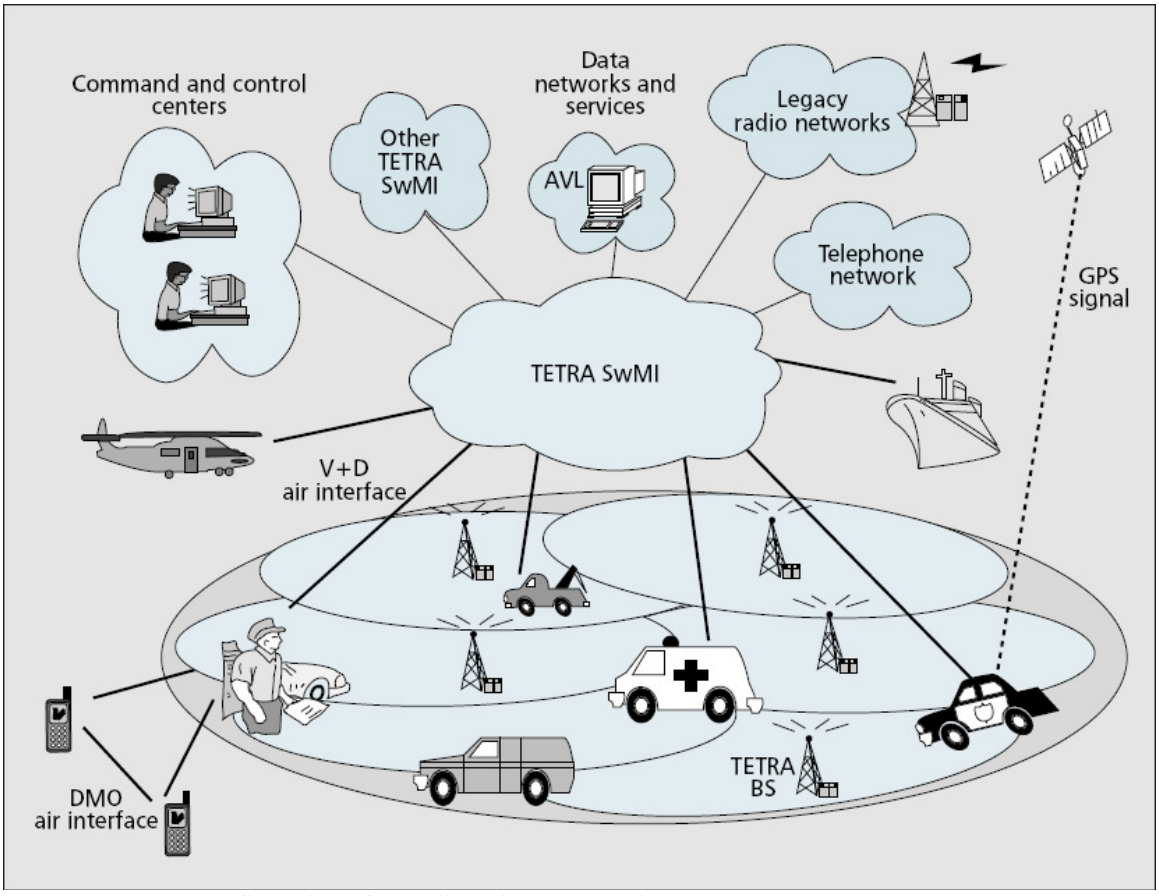

Figure 1: General configuration of a public Safety communication system based on the TETRA technology, copied from [Salk06]

The main TETRA services that are used within the public safety operational environment are the mission critical services, which are specified by TETRA [ETSI-TETRA]. TETRA

specifies two types of mission critical services: (1) Basic Service Set and (2) Supplementary Service Set. The basic service set consists of individual call, group call, acknowledged group call and broadcast call services. A supplementary service can modify or supplement a basic service. The supplementary service set consists of Pre-emptive Priority Call, Call Retention, Priority Call, Dynamic Group Number Assignment (DGNA), Ambience Listening, Call Authorized by Dispatcher, Area Selection and Late Entry services.

Several network scenarios can be applied in the public safety environment. [ODINI] specifies three network scenarios that can be used for this purpose: (1) tactical patch, (2) expand coverage, (3) migration to other networks.

1.2 Problem Statement, Requirements and Assumptions

Mission critical services are used by mobile users that can be located in different parts of the globe that are getting access to the public safety communication network using various wireless access networks, such as TETRA, UMTS, WiMax, LTE (Long Term Evolution). Within the public safety network, these wireless access networks are interconnected with each other using a core network via inter-system interfaces, see Figure 2.

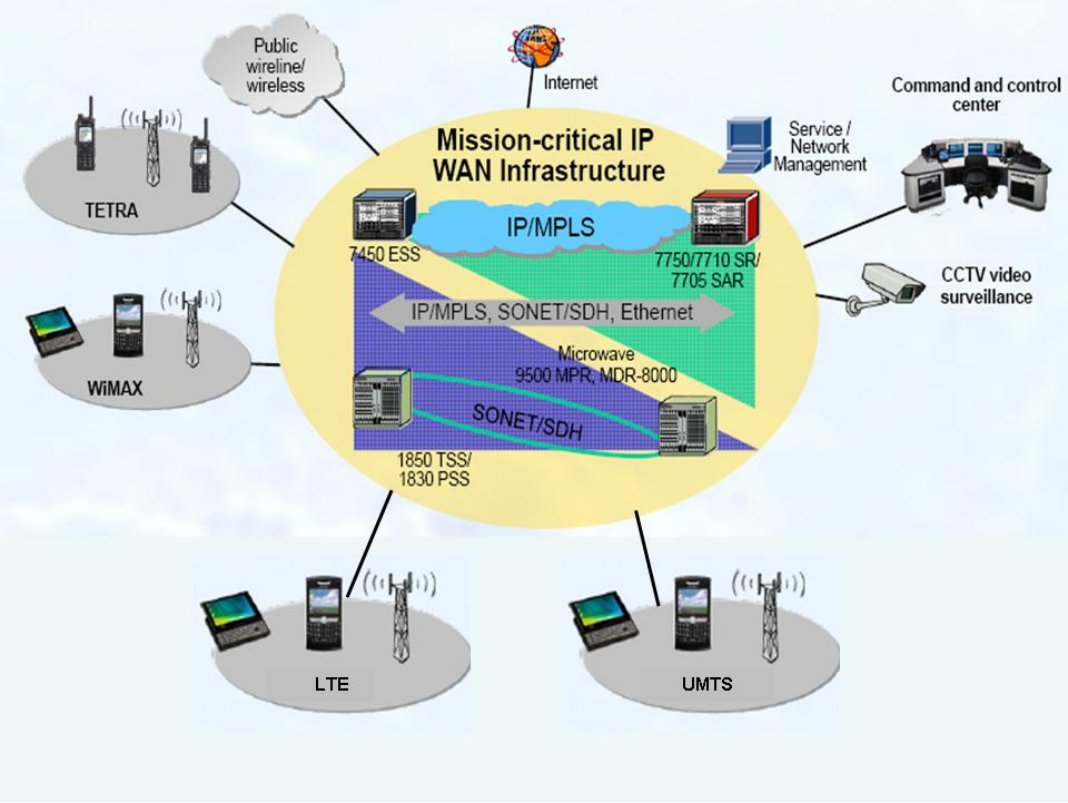

Figure 2: An example of a public safety network, based on [ODINI_slides]

A core network used to interconnect heterogeneous wireless communication systems that support mission critical group services needs to address issues such as multicast connectivity, mobility management, QoS support, security, etc. This section introduces the main requirements imposed by mission critical group services and the objectives used by this M.Sc. assignment in order to design a core network architecture that could solve the above mentioned issues.

1.2.1 Requirements

The main challenges associated with the operation of the core network are related to the strict performance requirements that are imposed by the mission critical services on the communication network. These performance requirements are specified in TETRA standards [ETSI-TETRA] and are the following:

QoS level: QoS is considered as a capability to support a certain performance level for different services or applications. QoS parameters include priority levels, bandwidth availability, latency, jitter, packet loss and pre-emption.

Priority levels: In [ETSI-EN-300392-10-10] it is specified that a typical TETRA scenario requires using 8 priority levels. Moreover, TETRA Association mentions, see [TETRA-A] that TETRA systems should be able to use at maximum 16 levels of priorities. Therefore, we consider that the core network architecture should be able to support at least 8 different levels of priorities.

Latency: is a time delay between the moment something is initiated, and the moment one of its effects begins or becomes detectable. In a network, latency is an expression of how much time it takes for a packet of data to reach the destination.

Jitter: is an expression of the variability over time of the latency across a network.

Packet loss rate: The rate of packets that are discarded when a device such as router or switch is overloaded and cannot accept any further data at a certain moment.

Pre-emption: is the right to purchase resources in advance of others. In the context of networking, pre-emption is used to differentiate between call types. For example, a pre-emption call could be supported by the TETRA network even when this network does not have available resources, by e.g., terminating ongoing (non preemption) calls.

Security: is the ability of a system to protect information and system resources with respect to unauthorized access and security attacks.

Reliability: is the ability of a system or component to maintain its functionality in a normal situation or under unexpected circumstances. Communication fallback methods are required to support reliability.

Mode of Communication: This requirement can be divided into two main types.
One is the unicast mode and another type is the multicast mode. Unicast represents the communication between one sender and one receiver over a network. Multicast represents the communication among (1) one sender and multiple receivers (one to many), or (2) among multiple senders and one receiver (many to one) or (3) among multiple senders and multiple receivers (many to many), over a network.
Another criterion that can be used to differentiate between modes of communication is by using the concept of unidirectional or bidirectional communication. Unidirectional communication is the communication mode in which the communication of user data (voice/speech, multimedia information, and data), between two (or more users) is accomplished only in one direction at a time. Bi-directional communication is the communication mode in which the communication of user data between two (or more users) is accomplished in two directions simultaneously.

Scalability: is a desirable ability of a system (communication network) to maintain its performance at a reasonable level when the amount of work load (e.g., number of users, or number of wireless access networks) is increasing.

Robustness: Robustness is the capability of a system (communication network) to resist and handle all kinds of failures and other type of stresses and pressures in unexpected environments.

Roaming and inter-system handover support: the ability of a communication network to support and maintain ongoing connections and communications of mobile users when they roam from one wireless access network (TETRA or other wireless access network) to another wireless access network (TETRA or other wireless access network).

One important challenge that needs to be solved is the design of a core network architecture that will be able to satisfy most of the performance requirements listed above.

1.2.2 Assumptions

Currently, TETRA is the only wireless technology that can provide mission-critical services. We assume that in the future also other types of wireless access technologies, such as WiMax, UMTS and LTE will be able to support such mission critical services.

Due to this fact, we assume that the wireless access networks are able to support the TETRA mission-critical services and that they are able to support the main Inter-System Interworking solutions provided by TETRA [ETS-300392-3-1], [ETSI-EN-300392-3-3] [ETSI-TS-100392-3-2]. However, the inter-system interworking solutions need to be more generic than the TETRA ISI solutions. Therefore several features need to be added on top of the TETRA ISI features.

We assume however, that the inter-system mobility solutions will not be based on the TETRA inter system mobility solutions, but on an IP based generic inter-system mobility

solution. This could for instance be Mobile IP [RFC3775] or Proxy Mobile IP [RFC5213]. We assume here that wireless access networks are able to transport new (non-TETRA) signaling messages, e.g. Proxy Mobile IP signaling messages.

1.3 Goal and Research Questions

The main goal of this Master of Science assignment is to specify, design and evaluate a core network architecture that is able to interconnect heterogeneous wireless communication systems using MPLS (Multi Protocol Label Switching) based IP networks for mission-critical group oriented communications.

In order to achieve the goal, several research questions have been defined:

(1) What are the application scenarios for mission-critical group communications?
(2) What are the requirements imposed by these application scenarios on the core network architecture used to interconnect heterogeneous wireless communication systems?
(3) Are there any existing standardized solutions that can fulfill these requirements?
(4) What are the core network architectural building blocks used for the interconnection of heterogeneous wireless communication systems applied for mission-critical group communications?
(5) How could this core network architecture be evaluated?

1.4 Research Approach

To perform the research required for this project, three research approaches are used: literature study, architecture design and scalability evaluation. In order to answer the first two research questions, literature study has been used on the TETRA standards and on the On-Demand Intelligent Network Interface (ODINI) public documentation. After performing the literature study for these two questions, we identify a list of mission critical services that can be divided into two categories: basic service and supplementary service. Moreover, three network scenarios have been identified. Based on the list of mission critical services and the three network scenarios, we derive a list of architecture requirements for interconnection of heterogeneous wireless communication systems. These requirements are already listed in section 1.2. For the third research question, a comprehensive literature study has been performed by studying IEEE papers, IETF Request for Comments (RFCs) and IETF Internet drafts. The outcome of this activity is a list of TETRA standards that are used to define ISI solutions, a list of IETF RFCs and internet drafts that can provide a generic ISI, generic mobility, multicast and Quality of Service (QoS) supported solutions. To answer the fourth research question, we define and design the architecture and the network entities that are used in the core network architecture, the functionalities supported by these network entities and the main message sequence charts used for the support of the mission group call communications. The message sequence charts are defined to show how the interworking is accomplished via the core network architecture. For the last research question, we evaluate the core network architecture with respect to scalability. In particular, several equations are

derived that can be used to derive the signaling load per signaling procedure, imposed by the main mission group call communication procedures, when the number of either wireless access networks or the number of moving users in increased.

1.5 Outline of the thesis

The rest of this thesis is organized as follows. Chapter 2 describes the mission-critical services, their network scenarios and requirements. Chapter 3 presents the existing MPLS based IP networking solutions. Chapter 4 specifies and designs the core network architecture for IP based interconnection of heterogeneous communication systems for mission-critical group oriented communications. Chapter 5 presents the core network evaluation activities from the point of view of scalability. Chapter 6 concludes this work and gives recommendations for further research.

Chapter 2: Mission Critical Services and their network scenarios

This chapter describes the main critical services and their requirements that are specified in the TETRA standards. Moreover, a description of the network scenarios that are supporting these services is given.

2.1 Mission Critical Services

Mission critical services, are supporting the communication between parties in public safety situations, including emergency situations, such as major incidents.

TETRA specifies two types of mission critical services:

- Basic Service Set: A basic service is a service that can provide information transfer between different user terminals. It consists of individual call, group call, acknowledged group call and broadcast call.

- Supplementary Service Set: A supplementary service is a service that can modify or supplement a basic service. It consists of Pre-emptive Priority Call, Call Retention, Priority Call, Dynamic Group Number Assignment (DGNA), Ambience Listening, Call Authorised by Dispatcher, Area Selection and Late Entry.

2.1.1 Basic Service Set

This subsection describes the main TETRA mission critical basic services, see [ETSI-EN-300392-3-3], [ETSI-TS-100392-3-2], [ETSI-EN-300392-3-4], [TETRA-A], [DuGi99].

2.1.1.1 Individual Call

Individual call is a point-to-point call that is established between two users. The calling user starts the call by sending a call-setup message to the user. The calling user will receive an acknowledgement concerning the call progress. The acknowledgement could be answered, unanswered or rejected etc.

2.1.1.2 Group Call

Among all the basic services, the Group Call is the most important one. This is a point-to-multipoint call established from one user towards more than one user. The call is set up immediately and the user who generates the call initially does not receive any

acknowledgement from other users. Basically, it allows a user to use the "Push to Talk" function to distribute information within one group. Other characteristics for this service are reliability, priority enabled ability, fast call set up time and optimal network loading capability [TETRA-A].

2.1.1.3 Acknowledged Group Call

The acknowledged group call is made only if the caller receives the acknowledgement from a group of involved users once they start to join the group call. The group members may be polled for presence. If the number of group member is insufficient, the call may be disconnected.

2.1.1.4 Broadcast Call

This is a typical communication way to make a group call. One user calls multiple users simultaneously. A broadcast call uses a unidirectional communication mode, since only the calling party can speak and the other participators will not send feedback to the calling party.

2.1.1.5 Data Services

TETRA can provide two categories of data services: Short Data Service and Packet Data Service.
The Short Data Service (SDS) is basically sending the short text message, which relies on the TDMA time slots. The SDS consists of the user defined short message and pre-defined short message. These two categories can be either individual or group short message.
The Packet Data Service can be divided into two types, namely: connection-oriented and connectionless service. The connection-oriented packet data service utilizes the virtual connections to deliver the data packets. The connectionless packet data service just simply transfers a data packet from one node to one or multiple nodes without using any logical connection.

2.1.1.5.1 Short Data Service

The short data service is a type of data service that is defined in [ETSI-EN-300392-3-4]. In general, it has the capability to send short messages in the form of point-to-point or point-to-multipoint communication modes.

This service imposes the following requirements: unicast, multicast and unidirectional communication modes and latency. An individual message is supported in the form of point-to-point. A group message is supported in the form of point-to-multipoint.

Multicast is required when the group message (point-to-multipoint) is used. Both individual messages and group messages are based on unidirectional communication. For the short data service, we want to receive a message immediately after the transmitter transmits it. Therefore, low latency is highly required. The short data service can support up to 254 characters [DuGi99].

2.1.1.5.2 Packet Data Service

The packet data service is supported based on TDMA (Time Division Multiple Access) technology. One TDMA time slot will support 4800 bits/s. For the data service, up to 4 TDMA time slots could be used. Utilization of multiple TDMA time slots can guarantee data throughput up to 19.2kbits/s [TETRA-A].

Two categories of packet data services have been defined. One is the connection oriented packet data service and the other one is the connectionless packet data service. The connection oriented packet data service is a data service that transfers packets in the point-to-point communication mode. As its name suggests, the logical connections between two users are set up and explicitly released. The connectionless packet data service delivers the packets either in the point-to-point or in the point-to-multipoint communication mode.

This service imposes the following requirements on the core network architecture: priority level, access and queuing priority, security, multicast, unicast and unidirectional communication mode. For packet data, multiple levels of priority should be provided for all packets sent from a mobile station. Higher priority packets should be sent before the lower priority packets. At the air interface, it is required to have different access priority on the uplink access channels so that the uplink access channels will first be made available to high priority messages [ETSI-TR-086-2]. The connection oriented packet data service requires the use of unicast communication. However, for the connectionless packet data service both unicast and multicast communication modes should be supported. The packet data service requires the use of the unidirectional communication mode, since sending a packet from one source node to another node or multiple nodes is a one way communication. The security requirements on Packet Data Optimized systems are defined in [ETSI-TR-086-3].

2.1.2 Supplementary Service Set

This subsection describes the main TETRA mission critical supplementary service set services. A supplementary service modifies or supplements a basic bearer service or teleservice or other supplementary services. Several procedures associated with TETRA supplementary services are given in [ETSI-EN-300392-1]. These procedures are:

1. **Provision** is an action that can make a service available to a user. Depends on whether the service is made available to all users or to an individual user, provision may be general (to all users) or pre-arranged (to an individual user).

2. **Withdrawal** is performed by the service provider to remove an available service from a user's access.
3. **Activation** is an action performed by the service provider or the served/authorized user to make a process to run.
4. **Deactivation** is an action that terminates the process started at the activation.
5. **Definition** is an action performed by the service provider or the served/authorized user to define or redefine parameters for a supplementary service.
6. **Registration** is an action performed by the service provider to identify certain authorized users to activate/deactivate/invoke/define/cancel/interrogate a supplementary service.
7. **Interrogation** is an action taken by the served/authorized user to obtain the useful information for a supplementary service.
8. **Cancellation** is an action performed by the served/authorized user so that an invoked supplementary service will be stopped.
9. **Invocation** is an action taken by the user or terminal to invoke the required service.
10. **Operation i**s the description of the normal operation.

2.1.2.1 Pre-emptive Priority Call

The supplementary service Pre-emptive Priority Call (SS-PPC) can differentiate a call from other calls by giving the call a high priority and the possibility of using resources that are at a certain moment used by other calls This means that in case of limited resources an emergency call can preempt and drop other (new or ongoing) calls that are assigned a lower priority.
The SS-PPC enables the user to have resources allocated, and disconnect the lower priority and lower Call Retention Value (CRV) ongoing calls. Note that the higher the call retention value a call has the lower the probability that this call will be dropped by a pre-emptive priority call.
Two types of pre-emption can be considered: (1) user pre-emption and (2) resource pre-emption. In user pre-emption the emergency call is selected above other competing and not yet active calls. In resource pre-emption the resources allocated to an active call are released and allocated to a SS-PPC.
In general, the calling user defines the pre-emptive priority level for the call, but the TETRA Switching and Management Infrastructure (SwMI) may modify this value. Note that SwMI represents the TETRA functionality that is responsible for the control of all switching and management activities within one TETRA domain.

When the required resources are not available for the SS-PPC call, SwMI should release resources of the oldest call which has the lowest SwMI CRV so the released resources can be provided to the SS-PPC call. SS-PPC is activated by the service provider upon provision and deactivated upon withdrawal [ETSI-EN-300392-10-16]. To invocate SS-PPC, the served user should be assigned a traffic channel and network resources. The oldest call with lowest (CRV) should be released. When there are any lower priority calls, resource pre-emption is used.

When the destination TETRA address is already involved in the existing call the pre-emptive priority call should have the ability to stop and pre-empt the call at the destination address. In fact, the user pre-emption consists of two steps: (1) SwMI decides whether the called user is involved or terminated. (2) If the SwMI does not terminate the existing call, the called user application will make a choice between the incoming call and the existing call. Assuming the SS-PPC call has higher priority than the active and ongoing call, there are two main categories to decide which priorities will lead to pre-emption. The difference between these two categories is whether we utilize the "user application" to decide pre-emption. We elaborate these by using the following tables.

Table 1: Priorities that cause user pre-emption from a lower priority call without user application decision

		Active call	
		Group	Individual
SS-PPC call	Group	Option 1: 3 and 4 Option 2: none	3 and 4
	Individual	3 and 4	3 and 4

Table 1 shows the priorities of the incoming SS-PPC calls that cause user preemption from a lower priority call, without a user application decision.

Table 2: Priorities on which user application decides pre-emption

		Active call	
		Group	Individual
SS-PPC call	Group	Option 1: 1 and 2 Option 2: 1, 2, 3 and 4	1 and 2
	Individual	1 and 2	1 and 2

Table 2 shows which priorities of the incoming SS-PPC call should use the "user application" to decide if the active call will be pre-empted or not.

Normal procedures contain activation, deactivation, definition, registration, interrogation and cancellation. Activation and deactivation are handled by the service provider once upon provision and withdrawal. Registration is not applicable. Interrogation is an optional function. SwMI will give a response to an interrogation which will contain activation state and priority value.

Despite the operating state of the SwMI, the served user should be provided a traffic channel and network resources

2.1.2.2 Call Retention

Supplementary Service Call Retention (SS-CRT) is an important service that allows the protection of calls against pre-emption. Call Retention enables the radio terminal users maintain their calls when the highest priority call is guaranteed. In TETRA system, every

call has a Call Retention Value (CRV). When the resources are required, the call which has the lowest CRV is pre-empted. In case that all the calls have the identical CRV, other criteria can be used to assign the resource to different calls. The criteria are the lifetime of the call, type of call, and user.

To use this service, provision and withdrawal of SS-CRT should be pre-arranged by the service provider. The provision of the service shall be on a per individual TETRA subscriber Identity (ITSI)/ Group TETRA Subscriber Identity (GTSI) basis [ETS-300 392-10-24]. Normal procedures contain activation, deactivation, registration, interrogation, invocation and operation. The SS-CRT activation and deactivation of is managed by the service provider upon provision and withdrawal, respectively. Registration is not applicable. Interrogation is provided by the SwMI. When interrogation is offered, a SwMI should support interrogation on a per individual user or group users basis. Note that an individual user is identified within TETRA using an Individual TETRA Subscriber Identity (ITSI) number and a group of users is identified by the Group TETRA Subscriber Identity (GTSI). Some information should be given: (1) whether interrogation is provided or not (2) default CRV (3) CRV range (4) applicable basic service.

SS-CRT is invoked by a calling user or by a called user to assign a CRV protection level to a call at the stage of call set up. From an implementation point of view, the network may invoke the SS-CRT automatically on behalf of the served user.

When the calling user starts a group call, he uses one of the values associated with his ITSI. The group controlling SwMI will choose the highest request value of CRV for the whole group call. Note that when more TETRA domains are involved in a group call, one of the participating SwMIs is selected to control the management of the group call. This SwMI is denoted as controlling SwMI.

Once the service is available, the served user should be able to activate and invoke SS-CRT at the stage of call set up, and should deliver the CRV for this call. Normally, the user has the ability to change the CRV after the call has been established.

Two categories of invocation have been defined, namely: invocation by a calling user and invocation by a called user. The calling user should have the ability to request SS-CRT as part of the initial call set-up. After receiving a call retention request, the SwMI should forward the CRV to the call destination. Once the call is completed, the originating SwMI should receive the called user CRV and set CRV value to the highest value. During the call, the calling user should have the ability to invoke SS-CRT when a change of CRV happens.

For the invocation by a called user, the called user should have the ability to request SS-CRT for protection in order to show a higher protection level than that of the incoming call. The request can be made independent of the calling user invoked SS-CRT [ETS-300 392-10-24]. Once a CRV of a higher value rather than the request CRV is accepted by the called user, the called SwMI will assign the highest value for that call and send the called

user requested CRV to the origin SwMI. During the call, the called user should have the ability to invoke SS-CRT when a change of CRV happens.

By using SS-CRT bandwidth availability can be up to a certain level guaranteed, since a call with a high CRV is protected against pre-emption [TETRA-A].

2.1.2.3 Priority Call

The Supplementary Service Priority Call (SS-PC) allows the infrastructure to assign network resources to calls based on the priority levels. Typical TETRA scenarios require 8 priority levels; see [[ETSI-EN-300392-10-10]. The priority level should be sent within the initial call set-up message. Alternatively, a default level is chosen by the network when user has not chosen a level [ETSI-EN-300392-10-10]. The priority level could be used to determine the priority of queuing for network resource. Another usage is to show the importance of the incoming call.

To use this service, the provision of SS-PC should be pre-arranged by the service provider. Withdrawal of service can be made temporarily or permanently by the system. SS-PC is provided based on a per TETRA identity number (ITSI/GTSI). Within a range of priority levels, a user will choose one priority level for a call. The priority level ranges are given once the provision of SS-PC occurs. This range can also be provided by the system.

Normal procedures contain activation, deactivation, definition, registration, interrogation and cancellation. Activation and deactivation are handled by the service provider once upon provision and withdrawal. According to the definition given in [ETSI-EN-300392-10-10], an authorized user is authorized to change the range of priority level of the served users' calls. A priority level is a value that is used to determine priority access to the network resource in case of congestion. From an implementation point of view, an authorized user can define the priority level or priority level ranges when SS-PC is supported. In addition, the authorized user who is able to define, activate or deactivate the priority level or priority level range, needs to be registered within the appropriate TETRA number range [ETSI-EN-300392-10-10]. For the interrogation, it is similar to the interrogation defined for SS-PPC. The infrastructure should provide interrogation in either local mode or remote mode. Compared with the information (activation state and priority values) provided to the user for SS-PPC, other necessary information are used that are the result of procedures, such as interrogation, assignment status, acknowledgement status from the user.

The served user should send the required priority level at the beginning of the set-up stage to invoke SS-PC. When no congestion occurs, the call can be established in a normal way. Once congestion occurs due to limited network resources, SwMI should compare all the intended calls' priority level and assign the network resource to the call that has the highest priority level. SS-PC can also be applied to a group call scenario. If the user within the group starts to call by dialing the Group TETRA Subscriber Identity

(GTSI), the corresponding priority level for the GTSI will be utilized. However, if the user does not belong to this group, his individual priority level will be used. Either the user or the TETRA network will choose a priority level for the intended call. Beside this, the network can also change the priority level dynamically.

SS-PC imposes the following requirements: priority level, bandwidth availability, bidirectional communication, unicast or multicast, priority requirements (access priority and queuing priority). Apparently, we need to support priority level to use this service. As already mentioned previously, [ETSI-EN-300392-10-10] specifies that typical TETRA scenarios require 8 priority levels. Other two relevant requirements would be access priority and queuing priority. In fact, we need to determine the order of access to the network resources which usually relies on the queuing priority. Since SS-PC could be divided into two types: group call or individual call, the unicast and multicast communication modes should both be supported. Moreover, bidirectional communication should be supported.

2.1.2.4 Dynamic Group Number Assignment

Supplementary Service-Dynamic Group Number Assignment (SS-DGNA) is especially useful when different users from various organizations want to communicate with each other. DGNA enables the user to create, modify, delete and interrogate groups [ETSI-EN-300392-10-22]. Two types of SS-DGNA have been defined. One type is the Call Related DGNA; and the other type is the Call Unrelated SS-DGNA. Call Related SS-DGNA is defined as a service to enable all the users of ongoing calls to be joined into one group. Call Unrelated SS-DGNA is defined as a service to create groups where a combination of individual users and groups are involved, which are not associated with active calls.

SS-DGNA is available to all TETRA users who have subscribed to this service. In the context of SS-DGNA, the definitions of affected user and authorized user have been defined. An affected user is an identified mobile station user to whom the group is assigned (added to) or de-assigned (removed from). Moreover, an affected user can use the assigned group numbers and interrogate group information based on group numbers.
An authorized user is a user who can manage SS-DGNA on numbers he is authorized to [ETSI-EN-300392-10-22]. The provision and withdrawal of this service is managed by the service provider. Normal procedures consist of activation, deactivation, definition, modification deletion, registration, interrogation, cancellation, invocation and operation. For call unrelated SS-DGNA, creation, modification and deletion of a group can be achieved by the authorized user. The authorized user will send a list of affected identities to the system. For call related SS-DGNA the system can form a new group by using the composition of the referenced call [ETSI-EN-300392-10-22]. An affected user and/or an authorized user can interrogate SS-DGNA number and its parameters. The information concerning the interrogation is listed in [ETSI-EN-300392-10-22]. Since the authorized user could modify the SS-DGNA numbers, the modification of the group should be notified to any added/removed member by invocation. When the group is de-assigned, the system will announce that the group identity is not valid anymore.

SS-DGNA imposes the following requirements: security, bi-directional communication, multicast, latency and reliability.

2.1.2.5 Ambience Listening

In general, the Supplementary Service Ambience Listening (SS-AL) allows the calling user to set a TETRA terminal into special type of voice call so that the TETRA terminal can transmit the information to the called user. The dispatcher can listen to ambient noise and dialogue via TETRA terminal. In this case, the TETRA terminal plays the role of the remote monitor to collect and distribute information concerning an unexpected situation.

From an implementation point of view, SS-AL may be invoked during a group call by a group call participating user. SS-AL could include a second listening party which could be either individual user or a group [ETSI-EN-300392-10-21]. Procedures of this service consist of provision/withdrawal, activation/deactivation, interrogation, invocation, operation and completion. The provision of this service needs to be pre-arranged by the service provider. SS-AL is activated by service provider upon provision and deactivated by service provider upon withdrawal. For the interrogation, users provide the following information to the authorized user: (1) whether SS-AL is invoked for TETRA identity or (2) not, where the listening party identity should be provided to the authorized user.

To invoke SS-AL call, a basic call set-up for individual call to the affected user should be adopted by the served user. The served user should also indicate a request for SS-AL. Once the request is accepted, the call set up attempt is forwarded to affect user's Mobile Station (MS). After the affected user's MS acknowledged the call set up request, SS-AL call set up can be provided. As an option, SS-AL may invocate a speech item during a group call. After the ambience listening, a call is set up or a speech item is invoked, and the MS should be put into a transmit mode. During this process, the microphone is open so that the dispatcher can listen to background noises and conversations within the range of the microphone [TETRA-A]. The completion of SS-AL is done when the served user clears down the ambience listening call or when affected user is to make or receive a call.

SS-AL imposes the following requirements: latency, unidirectional communication, multicast and security. Because it is an important service for those persons transporting important, valuable and /or sensitive material that could be hijack targets, security issue should be focused on. Since the affected user can participate to a group call, multicast communication happens when one dispatch should listen to many users. The SS-AL is used to listen to the conversation in the environment, which is using a unidirectional communication that occurs between the dispatcher and the environment.

2.1.2.6 Call Authorized by Dispatcher

The Supplementary Service Call Authorized by Dispatcher (SS-CAD) permits the dispatcher to verify a call request before it is allowed to proceed [ETSI-EN-300392-10-6]. The provision and withdrawal of SS-CAD is managed by the service provider.

The implementation options defined for SS-CAD are listed as follows: restricted basic service, restricted destination address, restricted source address and restricted area. In order to provide all these implementation options, the authorized user should provide the following common information to the service provider: the restricted basic services applicable to each implementation option, for which authorization should be given by the dispatcher and the dispatcher address where all requests for service should be diverted for approval. Other information that needs to be supplied for each individual implementation option is the identifications of each implementation option and gateway addresses. For all the implementation options, verification of the restricted users should be done before an SS-CAD definition is made. Once the authorized user generates an SS-CAD request, the service provider should notify the result of the request to the authorized user.

Normal procedures contain activation, deactivation, definition, registration, interrogation, invocation, operation and cancellation. SS-CAD is activated by the service provider upon provision and deactivated by the service provider upon withdrawal. The activation and deactivation may also be dealt with by authorized user. Once the provision occurs, the authorized user should be registered. The interrogation is supported by the SwMI. To give a feedback to the interrogation request, some information should be provided to the authorized user. This information consist of restricted user, activated or deactivated state of this service, applicable basic services, applicable destination address, applicable source address and restricted area [ETSI-EN-300392-10-6]. For invocation, two cases (outgoing calls and incoming calls) could be provided. When outgoing calls are generated from a restricted user, the SwMI will invoke SS-CAD once a call request is received. The SwMI should have the ability to determine whether to invoke the SS-CAD based on the calling party address, the called party address or area, and the basic service request. If the dispatcher authorizes the call without having diverted it to him, the dispatcher should give a confirmation of authorization to the SwMI [ETSI-EN-300392-10-6]. If the dispatcher does not authorize the call, then a rejection notification is sent to SwMI and the call is disconnected. The procedures also apply for the incoming calls.

The SS-CAD imposes the following requirements: uni-directional communication, because the dispatcher first has to verify a call request and afterwards this call can be established.

2.1.2.7 Area Selection

The Supplementary Service Area Selection (SS-AS) allows the user to choose a geographic area for outgoing calls. For the incoming call area selection, the incoming call is accepted only when the user is located in the defined area.

For this service, some concepts have been defined, such as authorized user, selected area, served user. In the context of area selection, the authorized user is the user who can

define areas. The served user is the originator of the call who uses SS-AS to set up a call within a certain area. Selected area is the defined area that is invoked by a served user to establish a call.

The procedures of this service contain provision, withdrawal, activation, deactivation, definition, registration, interrogation, cancellation, invocation and operation. Provision and withdrawal of service is handled by the service provider. Among these procedures, the interrogation is an important procedure. When it is started by the served user, the response to the interrogation will contain the parameters such as service provided and areas availability. When the interrogation is done by the authorized user for an ITSI or GTSI, the response for the interrogation should contain a list of ITSI/GTSI that is used for defined areas [ETSI-EN-300392-10-8]. The invocation of this service is based on a call per call basis. SS-AS can improve network loading and spectrum efficiency by limiting operating area for a certain amount of group calls.

SS-AS imposes the following requirements: bandwidth availability, bi-directional communication and scalability. Since area selection is helpful for improving network loading and spectrum efficiency, bandwidth requirements should be supported.

2.1.2.8 Late Entry

Supplementary Service Late Entry (SS-LE) is an important service to guarantee the multipoint speech call. The SwMI should send the late entry message along the network to allow the group members to join the conversation. Actually, it is considered to be an air interface feature rather than a service [TETRA-A].

For this service, several concepts have been defined in [ETSI-EN-300392-10-14], such as authorized user, bearer service, forced late entry, late entry acknowledgement, late entry broadcast, late entry paging and multipoint call.

Among all of them, an authorized user is the identified user who can define the SS-LE parameters. Multipoint call is the call that can support point-to-multipoint communication. Late entry acknowledgement represent the indications that are sent by the SwMI to announce that anyone who wants to join the call have to notify his participation to the SwMI. Late entry broadcast is an indication sent by the SwMI to all the intended participators that are not active in the call. These participators are informed that they could join the current voice communication. Late entry paging is the indication sent by the SwMI to inform all the intended participators that they a communication channel have to be allocated for them in order to join the current call.

The procedures of this service contain provision, withdrawal, activation, deactivation, definition, registration, interrogation, cancellation, invocation and operation. As usual, the service provider will be in charge of issues like provision, withdrawal, activation and deactivation. For the definition and removal, some important information should be provided by the authorized user. This information consists of group identity, LE definition/removal, LE used over ISI (Intersystem Interface), Call behavior, Basic service

type and Repetition rate. Registration is utilized to identify the authorized users. A list of GTSIs should be given to the authorized user [ETSI-EN-300392-10-14]. Invocation and operation is performed by the network after the set up is accomplished. Operation mainly concerns the relevant information about the group call and the network resources' availability.

This service imposes the following requirements: bandwidth availability and multicast communication. For this service, since we need to consider the network resource availability, proper bandwidth allocation will make sure that the late entry is successful for the late comer. Multicast should be supported since LE is carried out based on the existing group call. SwMI will use late entry broadcast to tell the members of a multipoint call that they could participate in the call if required.

2.2 Network Scenarios

In this subsection three types of TETRA network scenarios are described, needed to support the TETRA mission critical services, see [ODINI], when multiple wireless access networks are interconnected by one shared core network.

2.2.1 Tactical Patch

This network scenario is representing a scenario where communication between mobile stations (MSs) located within different wireless access networks is supported and where it is assumed that during a certain call each MS participating in this call remain in the coverage area of one wireless access network (i.e., assumed that roaming between different wireless access networks is not supported).
Two application scenarios can be distinguished within the tactical patch network scenario. The first application scenario is the cross-border cooperation of public safety officers, see Figure 3. Alternatively, two different regions within a big country can also use this scenario.

Basically, two separate networks are presented in Figure 3, which are interconnected using an IP based core network. One network is used for each country. Public safety officers from two different countries can form a group communication team by using e.g., push-to-talk voice services.
When e.g., more police officers are involved in this scenario, a hierarchical driven organization can be used. It means that the main officer may only supervise the foreign police force. In other words, only one control room will be adopted. As we can see from Figure 3, both group calls and individual calls can be supported by this scenario.

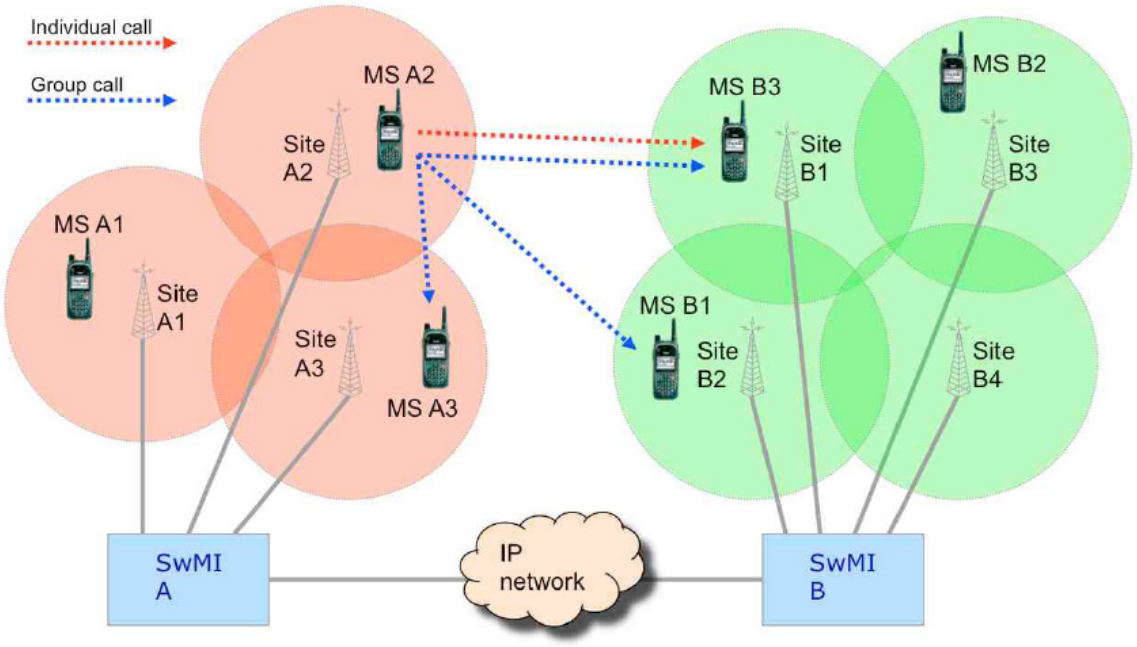

Figure 3: Tactical Patch: Cross-border cooperation, copied from [ODINI]

The second application scenario is the interconnection of overlapping networks from different organizations, see Figure 4.

Inter-agency cooperation is used when users located in different radio networks want to communicate with each other during an incident. The main officer will be in charge of authorization for cooperation. Typical usage schemes of inter-agency cooperation are listed below [ODINI]:

1. Cooperation of private fire brigades with their public counterparts for a fire accident. Private fire brigades are also hired by airport, hotel, tunnel operators and large industrial plants.
2. Communication between security personnel and public safety officers in the control room. This usage can be deployed at stadium, airport and shopping malls.
3. Communication between armed forces and police officers.
4. Communication among fire brigades, police and medical services. When a large-scale incident or disaster happens, these three parts can cooperate with each other to rescue people.
5. Connection between a deployed system and a regional or countrywide network to increase the capacity during a large-scale incident or disaster.

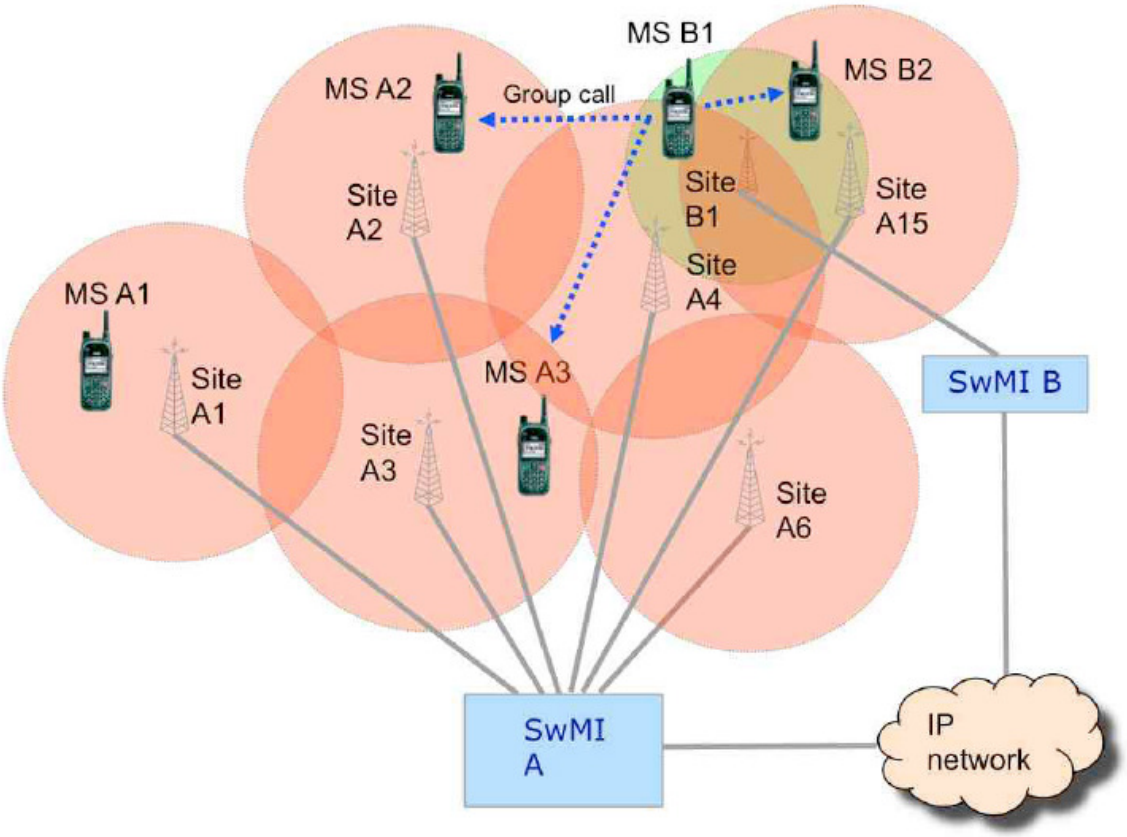

Figure 4: Tactical Patch: Inter-agency cooperation, copied from [ODINI]

From Figure 4, it can be noticed that only group calls are supported by this scenario.

2.2.2 Expanding Coverage

Expanding coverage of a current network needs to combine multiple radio networks in order to perform the functionality of a single radio network, see Figure 5. The main challenge of the expanding coverage is the integration of different radio networks that are based on proprietary architectures.

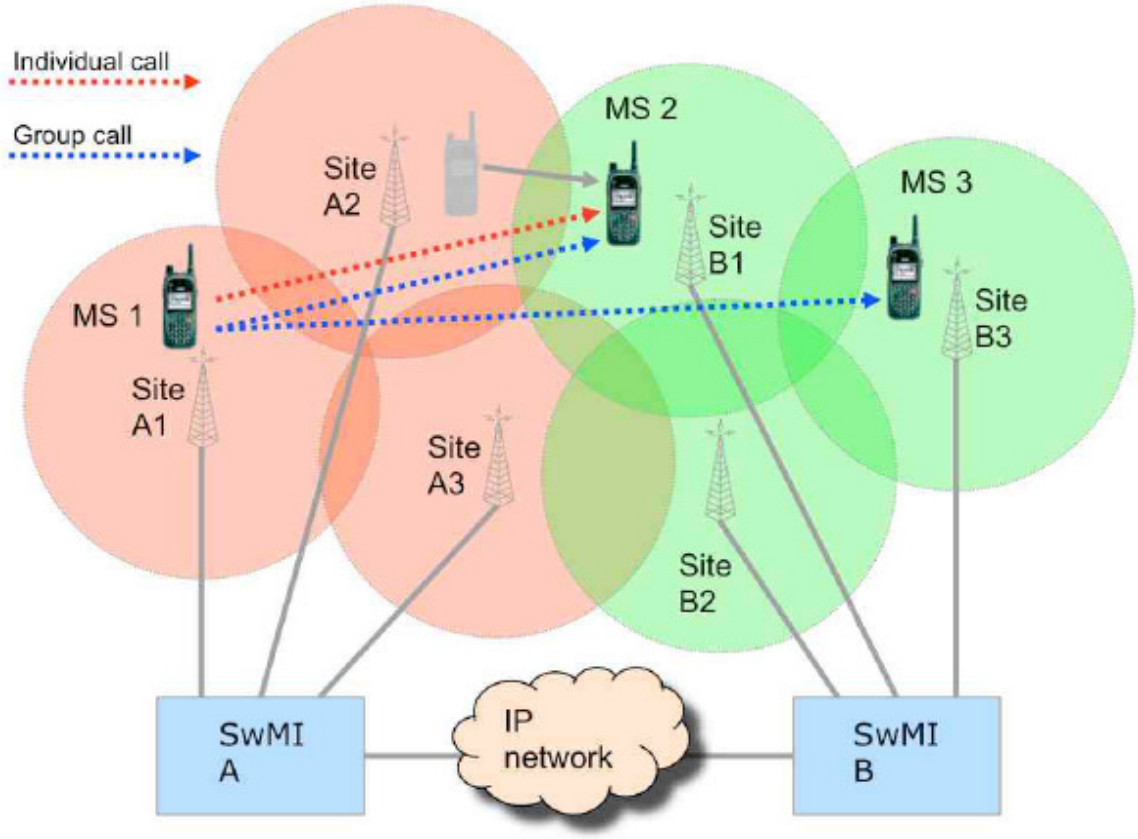

Figure 5: Expanding Coverage, copied from [ODINI]

This scenario mainly differs from the Tactical Patch scenario on the fact that MSs can roam to other wireless access networks.
In this scenario, suppose one city has two parts: part A and part B. The SwMI in network A serves 3 sites and the SwMI in part B serves 3 sites as well. Allowing seamless roaming between the two networks, the SwMIs should have the same Mobile Country Code (MCC) and Mobile Network Code (MNC). MCC is a number that is used to indentify the country where the subscriber belongs to. MNC is a number that shows which operator the mobile user is subscribing to.

2.2.3 Migration to other network

This scenario is similar to the expanding coverage scenario, with the main difference that it is not required to combine multiple radio networks in order to perform the functionality of a single radio network, see Figure 6. Similar to roaming in GSM (Global System for Mobile communication), when a mobile station moves out of its home network coverage, it will search for other radio networks. Once the foreign network informs that roaming is available, the mobile station will register as a visitor in this foreign network.

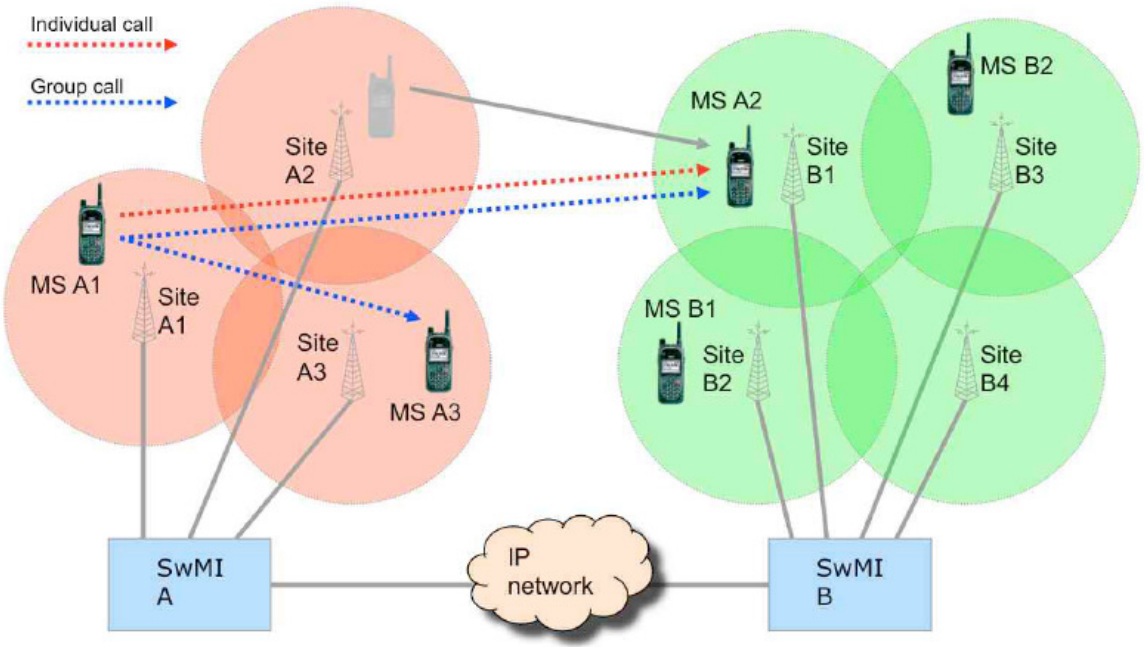

Figure 6: Migration to other network, copied from [ODINI]

A typical application example that uses this scenario is the cross-border operation of public safety officers. Police officers are able to communicate with policemen that are roaming within one country or are moving across country borders. The cross-border operation will become more and more important in mission-critical networks.

Chapter 3: Existing Standardized solutions used in IP based core networks

This chapter describes the main standardized solutions that can be used in an IP based core network to support the requirements discussed in Chapter 2. The main technology that will be used within the core network is MPLS [RFC3031] and MPLS multicast [RFC5332].

Regarding QoS support, there are several solutions defined. Such solutions are: Resource Reservation Protocol (RSVP) [RFC2205], RSVP-TE [RFC3209], Integrated Services (IntServ) [RFC1633], Differentiated Services [RFC2475], Next Steps in Signaling (NSIS) [RFC4080], [RFC5971], [RFC5974].

Regarding IP multicast routing, two options are identified by the IETF:
Option 1: Use the Internet Group Management Protocol (IGMPv3) [RFC3376] together with the Host Extensions for IP Multicasting [RFC1112] and the IGMP/MLD-based forwarding [RFC4605].
Option 2: Use the Internet Group Management Protocol (IGMPv3) in combination of Host Extensions for IP Multicasting [RFC1112] and a certain type of IP multicast routing protocol, for instance Protocol Independent Multicast-Sparse Mode (PIM-SM) [RFC4601].

Regarding mobility management, the main solutions that are identified are: Mobile IPv4 [RFC3344], Mobile IPv6 [RFC3775], Proxy Mobile IP [RFC5213], [RFC5844], Base Deployment for Multicast Listener Support in PMIPv6 Domains [ScWa10].

Regarding security support, the main solutions that are identified are: MPLS security architecture [RFC5920], IP Security Architecture (IPSec) [RFC5213].

In this chapter, some existing TETRA based standardized solutions are described, which can be used to define generic inter-system interworking solutions used in core networks. QoS support and IP multicast solutions are addressed since QoS and multicast communication have been identified as being the most important architecture requirements.
Furthermore, some generic inter-system mobility solutions are briefly discussed. The security support within MPLS network will be discussed at the end of this chapter.

3.1 TETRA Inter-System Interface

The inter-system-interface (ISI) is a way of communication where users from one TETRA system can communicate with mobile users from another system (either TETRA or others). One specific TETRA network probably needs to interface and communicate with different types of networks, such as: another TETRA network, a GSM network, a GPRS (General Packet Radio Service) network, a UMTS network or a Tetrapol network

[TETRAPOL], etc. ISI is the ability of multiple networks to cooperate and provide services. In this section several TETRA ISI solutions are discussed that are able to support the Inter-System Interface for (1) individual calls, (2) group calls, (3) mobility support and (4) short data service.

3.1.1 TETRA Inter-System Interface Individual Call

When a calling user setups an Individual call, an Additional Network Feature Inter-System Interface Individual Call (ANF-ISIIC) [ETS-300392-3-1] should be invoked to extend this call over the ISI, see Figure 7.

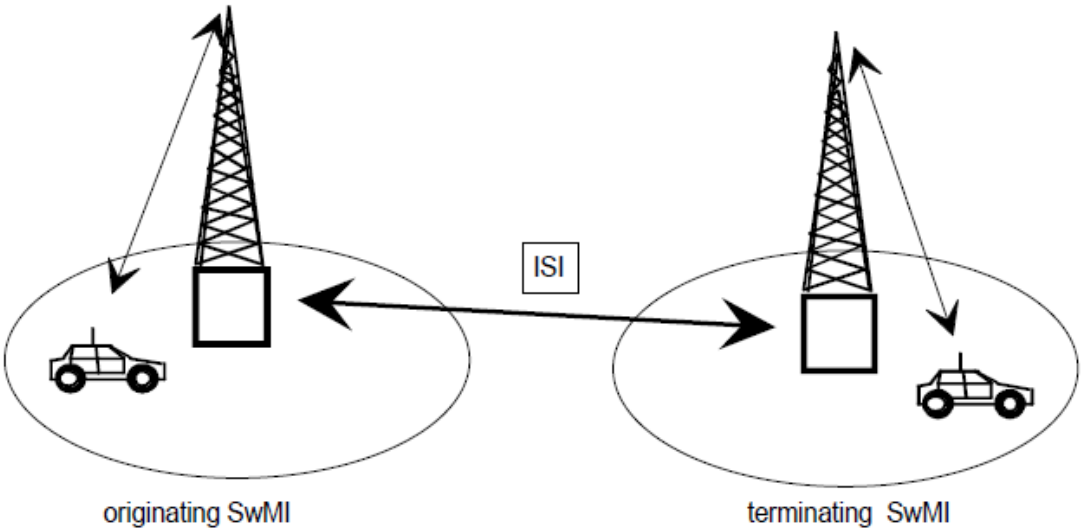

Figure 7: Individual Call Configuration

ANF-ISIIC enables one mobile user at one Switching and Management Infrastructure (SwMI) to set up the individual call to another mobile user at another SwMI. ANF-ISIIC operates at the ISI of both SwMI call control applications. During the duration of the call, the signaling messages need to be transported between one TETRA SwMI and another TETRA SwMI, which is handled by the ANF-ISIIC.

3.1.2 TETRA Inter-System Interface Group Call

The group call shall be available or controlled by using the provision (setup) and withdrawal (release). Provision is an action that can make a service available to a user. Withdrawal is performed by the service provider to remove an available service from a user's access. The Additional Network Feature Inter-System Interface Group call (ANF-ISIGC) [ETSI-EN-300392-3-3] shall be permanently activated on provision and deactivated on withdrawal. The ANF-ISIGC should provide services to SwMI Call Control applications. There are 4 generic service primitives defined for the ANF-ISIGC services: request, indication, response and confirm, see Figure 8.

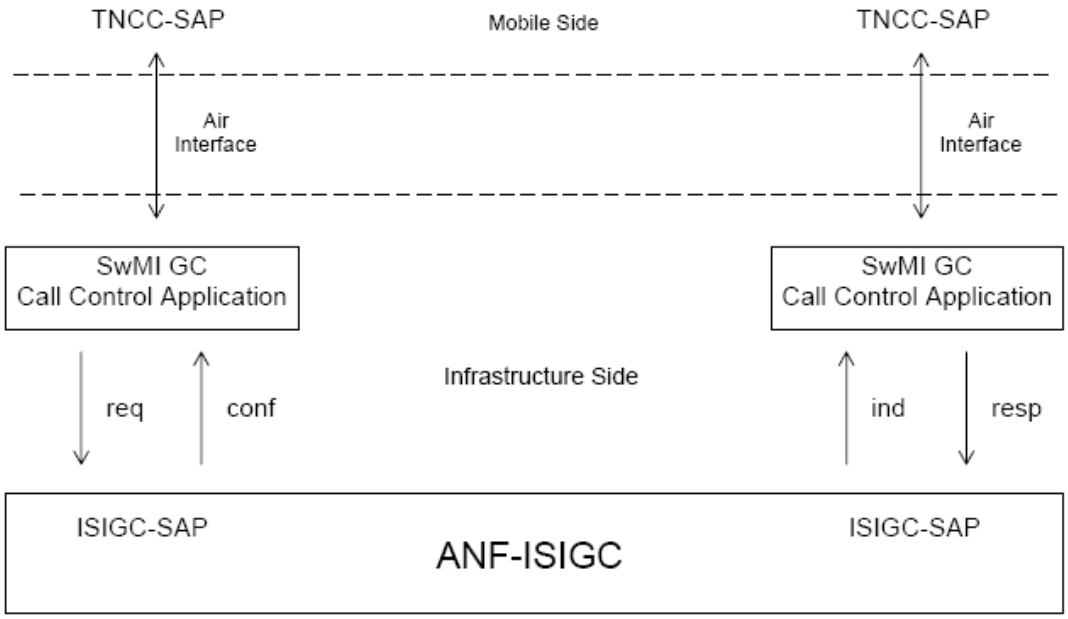

Figure 8: ANF-ISIGC stage 1 service model [ETSI-EN-300392-3-3]

To specify the set up steps of a group call, several definitions have been given in [ETSI-EN-300392-3-3]. Controlling Switching and Management Infrastructure (CSwMI) is a SwMI which can setup and maintain a call between two or more SwMIs. In Figure 9 a group call configuration is shown where an originating SwMI is the home SwMI of the group. An Originating SwMI (OSwMI) is the one where the call originates. The Participating TETRA SwMI (PSwMI) is the SwMI that only participates in the call and it is the one where the call is terminated. The group call can be initiated at the originating and the controlling TETRA SwMI.

ANF-ISIGC should be invoked when a group call request has been received by the originating SwMI. The ANF-ISIGC entity should analyze the originating Mobile Station identity ITSI (Individual TETRA subscriber Identity) and the destination group identity GTSI (Group TETRA Subscriber Identity). ITSI is a TETRA Subscriber Identity assigned to an individual TETRA user. GTSI is a TETRA Subscriber Identity assigned to a group. The request for group call establishment should contain the information as follows: (1) basic service information qualifying the bearer capability (2) called party identity specified by the GTSI (3) transmission control information (4) priority of the call. After the analysis of the called group profiles, the ANF-ISIGC entity should be notified about the analysis result. If the call is accepted, the ANF-ISIGC entity should analyze the called group identity. The set-up of a group call may involve more than one OSwMI. But it only needs one CSwMI. OSwMI could indicate that it is ready for the call connection.

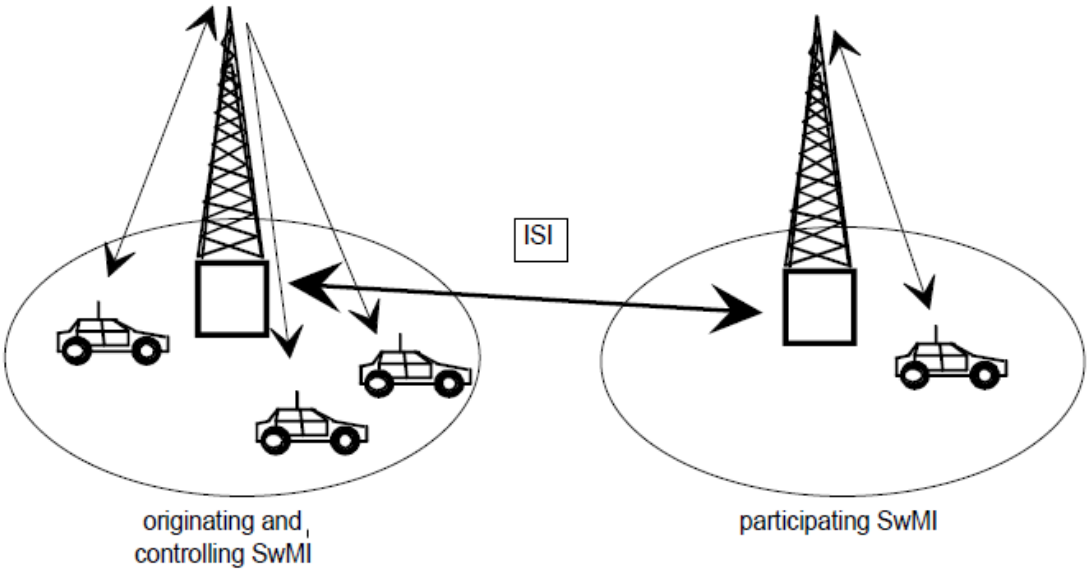

Figure 9: Group Call Configuration [ETS-300392-3-1]

Another way is to establish a group call at a participating PSwMI. In Figure 10 another group call configuration is shown where an originating SwMI of a group call is not the group home SwMI. In this case the originating SwMI becomes a participating SwMI.

When the controlling SwMI has been determined, the ANF-ISIGC CSwMI entity should analyze the call set-up information that is given in the forwarded set-up request and the location information of all group members. The invoked SwMIs Call Control application should check whether the network resources are available for the group call and for the group members that are using the SwMI. The network resources (air interface, mobile and infrastructure resources) should be reserved to perform a group call. Depending on the content of the request and on the available resources, the PSwMI can decide whether it is ready to be connected by the OSwMI. The invoked PSwMIs should give a set-up response back to the controlling SwMI clearly indicating the modes of operation, which are used to assign the available resources. There are two modes of operation for a participating TETRA SwMI to allocate resources during the call maintenance: permanently allocated resources and temporary allocated resources. The set-up response can also point out whether the group call is valid and what kind of communication type the SwMI can support (e.g. normal, acknowledge or broadcast call). Otherwise, if the invoked SwMI cannot accept the indicated service, then the call needs to be rejected. The set-up responses should be sent to the controlling SwMI The controlling SwMI Call Control application will determine whether the call can be setup as a complete or part of the group call. If the group call is accepted, the originating SwMI and participating SwMI should be notified to connect the participating members of the group call.

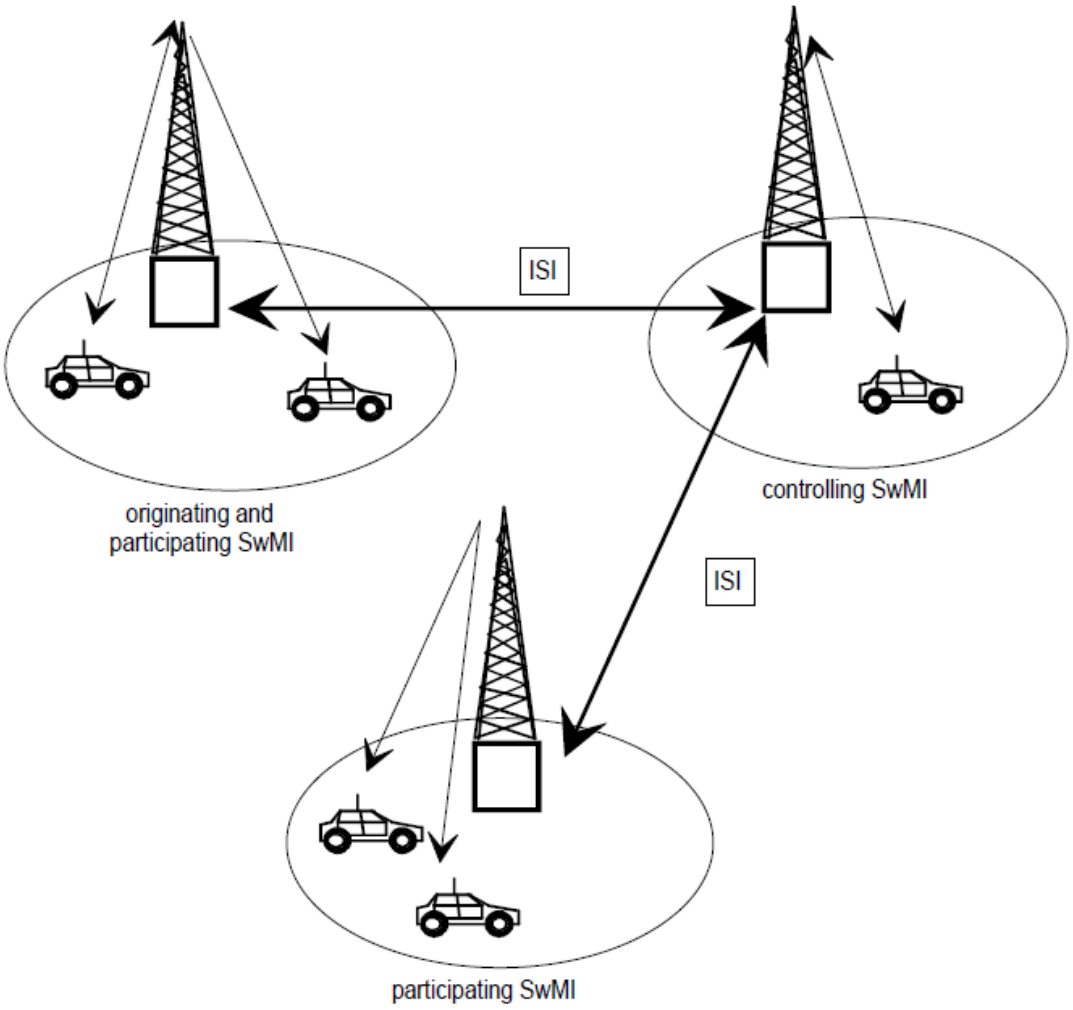

Figure 10: Group Call Configuration [ETS-300392-3-1]

3.1.3 TETRA Inter-System Interface Mobility Management

The ANF ISI Mobility Management (ANF-ISIMM) [ETSI-ETS-300392-3-5] specifies additional Mobility Management Services to be supported by the SwMIs. The ANF-ISMM complements the intra-SwMI-Mobility Management (intra-SwMI-MM) services and provides the following services: (1) migration and restricted migration, (2) individual subscriber and group profile registration and update, , (3) group attachment/detachment, (4) de-registration, (5) individual subscriber and group database fault recovery, (6) authentication, (7) security key management and distribution [ETSI-ETS-300392-3-5].

3.1.4 TETRA Inter-System Interface Short Data Service

The short data service is supported by Additional Network Feature-Interworking at Inter-system Interface Short Data Service (ANF-ISISD) [ETSI-EN-300392-3-4].

The ANF-ISISD enables short data and status messages to be set-up and transferred between two users that are registered in two separate TETRA networks [ETSI-EN-300-392-3-4]. The short data service should be provided by a single SDS (Short Data Service) functional entity at the TNSDS-SAP. The short data functional entity consists of the following services [ETSI-EN-300392-2]:

1. User defined short message reception and transmission for both individual and group message
2. Pre-defined short message reception and transmission for both individual and group message

3.2 IP Multicast routing and QoS supported solution

This section will mainly describe the current standardized IETF IP multicast routing and QoS supported solutions that can be applied in core networks. First the QoS solutions are discussed and after that several multicast routing solutions are presented.

3.2.1 RSVP

Resource Reservation Protocol (RSVP) is a resource reservation setup protocol that can be used by the Integrated Service [RFC1633] model. RSVP is used by a receiver of a multicast or unicast data flow to request specific QoS for application data streams or flows [RFC2205]. Every router can use RSVP to deliver QoS requests at all nodes along the communication data paths among sender and receivers. These requests will make sure the resources are reserved at each node located on the communication data path. All the reserved resources in every router are maintained in the form of “Soft State”. Soft state is a state that is maintained by using periodic refresh messages, which contains all kinds of information concerning traffic flow such as routing initiator, destination, routing message, resource information etc. In order to guarantee QoS, a set of mechanisms called the “traffic control” is adopted in each RSVP aware node. Traffic control is achieved by mainly 3 features, namely: a packet classifier, admission control and a packet scheduler.

3.2.2 RSVP-TE

RSVP-TE [RFC3209] is an extension of the RSVP protocol for traffic engineering. It is used to establish Label Switched Paths (LSPs) in an MPLS network to meet the traffic engineering requirements. Furthermore, the extended RSVP-TE protocol supports the instantiation of explicitly routed LSPs, with or without the support of resource reservations. Additionally, RSVP-TE supports smooth rerouting of LSPs, differentiation based on 8 priority classes, preemption, and loop detection.

RSVP-TE supports the management of LSP tunnels, which allow the implementation of a variety of policies related to network performance optimization. An example of this is that LSP tunnels can be automatically or manually routed away from network failures,

congestion, and bottlenecks. In addition to that, RSVP-TE is able to establish multiple parallel LSP tunnels between two nodes, and traffic between these two nodes can be mapped onto the LSP tunnels according to local policy.

3.2.3 MPLS and GMPLS

In an MPLS domain, see Figure 11, two main types of routers are used, the Label Edge Router (LER) that is located at the boundary (edge) of the MPLS domain and the Label Switching Router (LSR) that is located within the MPLS domain, see [RFC3031]. A Label Switched Path (LSP) consists of one or more paths that are passing through one or more LSRs and are starting at ingress LER(s) and ending at egress LER(s). A LER is a router that operates at the edge of an MPLS domain. LER is able to classify incoming packets in Forwarding Equivalence Classes (FEC). These FEC classes are used to specify how packets belonging to them should be treated within the MPLS domain. In addition to this the LER is able to include/extract a label from an IP packet. In MPLS, a label is a short and fixed length value that is utilized to indentify a FEC and it has a local (one hop) meaning. Therefore, a label is swapped with the new one at each LSR. In particular, a packet is sent together with the label that is associated with FEC and at following LSR hops, the label is swapped with a new label and the packet is sent to the next hop. Therefore, each LSR has to dynamically maintain a table that will be used during the label swapping process. Each row of this table will specify the LSR's input port, the incoming label, the LSR output port and the outgoing port.

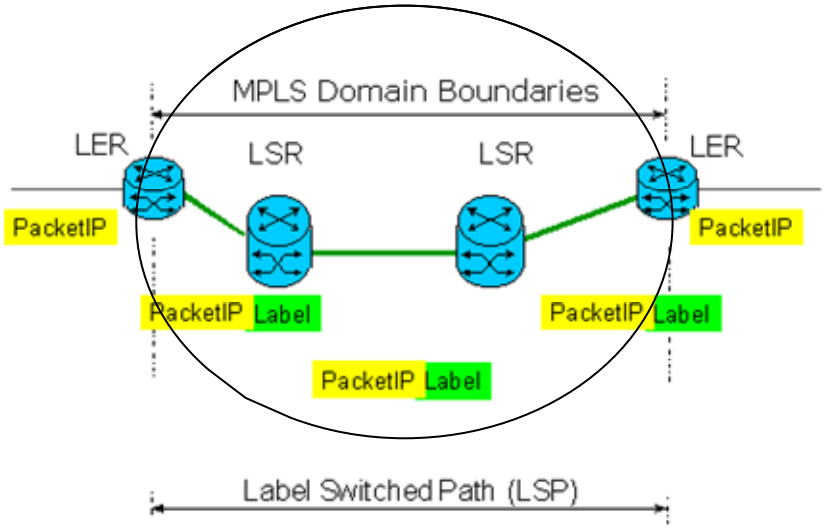

Figure 11: MPLS architecture

GMPLS (Generalized Multiprotocol Label Switching) [RFC3945] extends MPLS to encompass time-division, wavelength (lambdas), spatial switching. GMPLS enhances MPLS by completely separating control and data planes of various networking layers. The GMPLS architecture divides the control plane into two parts: the signaling plane and the routing plane. The signaling plane contains the signaling protocols and the routing plane contains the routing protocols. Other main differences between GMPLS and MPLS are listed as follows: (1) In GMPLS, bi-directional LSP is supported while in MPLS only

unidirectional LSP is supported. (2) In GMPLS, Label assignment can be done in two ways: downstream-to-upstream label assignment and upstream-to-downstream label assignment, while MPLS only supports downstream-to-upstream label assignment. (3) In MPLS, a label is attached to a packet. In GMPLS, a virtual label is used and the label can also be a certain channel or port.

3.2.4 MPLS Multicast Encapsulations

In the context of the 'Next Hop Label Forwarding Entry' (NHLFE) [RFC3031], once an MPLS packet arrives, its top label will be mapped to an NHLFE. This packet will be sent to the next hop determined by the NHLFE. In [RFC5332], a particular MPLS label called multicast label is defined. In the context of NHLFE, the packet will be duplicated at a set of hops that are defined by the NHLFE. A label becomes a multicast label as long as the packet duplication and delivery to all the members those are located in the set of next hops happens.

In [RFC3032], two data link layer codepoints have been defined for MPLS: one codepoint shows that an MPLS unicast packet is carried by the data link layer frame, and another codepoint shows that an MPLS multicast packet is carried by the data link layer frame. Since the NHLFE can find out whether the top label is a multicast label or not, the data link layer codepoints do not need to perform this function. Also the deployment of data link layer codepoints has not been done yet.

It is known that implementation for MPLS multicast based on the [RFC3032] cannot interoperate with implementations that rely on the concept of "multicast label". The possible implementations that are in favor of data link layer codepoints actually lack the control plane. [RFC3032] also specifies a mechanism to carry a MPLS packet in an Ethernet multicast frame.

[RFC5332] describes a method to support multicast in MPLS. There are two types of label binding in MPLS. Considering one Label Switching, Router R1 sends a labeled packet to R2. R2 will determine its Forwarding Equivalence Class (FEC). If R2 sends a label binding to R1, this type of label binding is called downstream-assigned label binding. See Figure 12.

Figure 12: Downstream-assigned label binding

If R1 sends a label binding to R2, this type of label binding is called upstream-assigned label binding. See Figure 13.

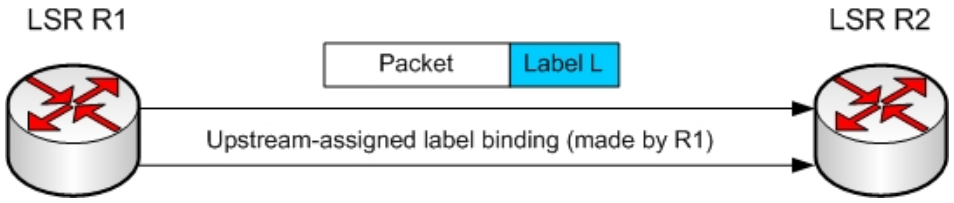

Figure 13: Upstream-assigned label binding

If the third party R3 does the label binding and sends label bindings to R1 and R2, this case is also considered to be upstream-assigned label binding. See Figure 14.

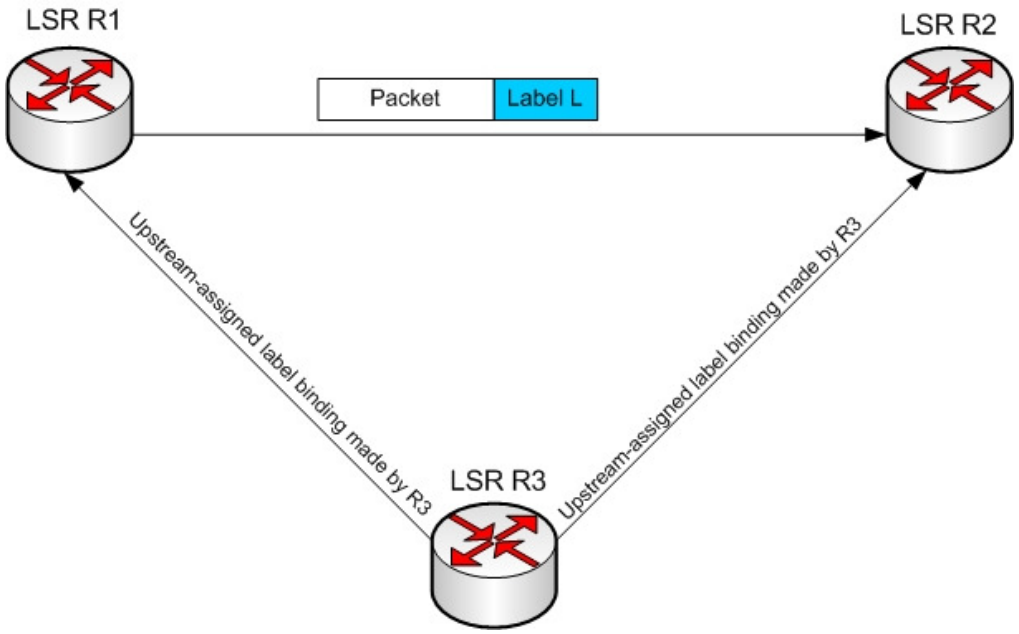

Figure 14: Upstream-assigned label binding made by Router 3

Three mechanisms have been defined to transmit an MPLS packet when Upstream LSR (Ru) and Downstream LSR (Rd) are located at one LSP. Ru and Rd can transmit MPLS packet to each other. These three mechanisms are listed below, see Figure 15.

1. By putting the MPLS packet in a data link layer frame and transmitting the frame

2. By transmitting the MPLS packet through an MPLS tunnel, i.e. by pushing an additional label (or labels) onto the label stack, and then invoking mechanism 1, or

3. By transmitting the MPLS packet through an IP-based tunnel, and then invoking mechanisms 1 and/or 2.

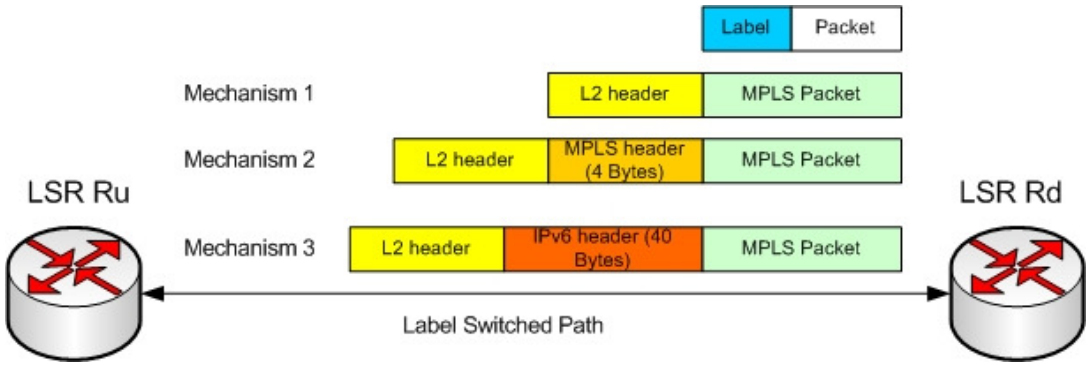

Figure 15: Three mechanisms for transmitting an MPLS packet between two LSRs

In fact, an MPLS packet can be transmitted via a data link, via an MPLS tunnel or an IP tunnel. According to the mode of communication, there are three different types of data link or tunnel:

1. Point-to-Point. A point-to-point data link or tunnel means that two systems are located at two sides of the data link or tunnel. The transmission is done from one party to another party.

2. Point-to-Multipoint. A point-to-multipoint link or tunnel implies multiple systems are involved, and only one party can be the transmitter of the data link or tunnel, and the remaining parties are the receivers.

3. Multipoint-to-Multipoint. A multipoint-to-multipoint link or tunnel implies n systems. Any of the n systems can transmit on the link or tunnel, and the remaining systems will be the receivers.

3.2.5 Differentiated services (Diffserv)

Differentiated Services (DiffServ) [RFC2475] is an IP based QoS architecture that specifies a simple and scalable mechanism to classify and schedule network traffic in order to provide QoS support within one administrative domain. This architecture supports two main types of network entities: (1) edge nodes, which are nodes located at the edge of the Diffserv domain and (2) interior nodes, which are nodes located within the Diffserv domain.
Packet classification is performed by using DiffServ codepoints (DSCP) that are carried by data packets. Each DSCP is associated with one Per Hop Behavior (PHB), which specifies how a router should treat, schedule and forward a packet that carries a certain DSCP. It is important to emphasize that DiffServ does not provide end to end QoS support.

3.2.6 Integrated services (IntServ)

Integrated Services (IntServ) [RFC1633] is aimed at supporting end-to-end QoS to be provided to applications. Intserv specifies the features that all routers (nodes) located in an end-to-end communication path (from sender towards receiver) need to support for the realization of the end-to-end QoS support. IntServ mainly relies on admission control and resource reservation. The IntServ model consists of three parts: (1) Resource setup protocol: It dynamically reserves the network resources to meet the requirements of special traffic flow. The main signaling protocol used for this purpose is the Resource Reservation Protocol (RSVP) [RFC2205], (2) Flow Specification: It is a set of reserved resources that are utilized to support QoS of one specific traffic flow. (3) Traffic Control: In the network equipment of each node, some functionalities can classify and schedule data packets and control and manage the network resources to support specific QoS.

3.2.7 Scalable CORE

The last QoS solution we present here is Scalable CORE proposed in [StZh99]. This work is based on Dynamic Packet State (DPS). DPS is a technique to provide scalable network services in a network domain. DPS can guarantee services with levels of flexibility, utilization and assurance similar to the per flow approaches. SCORE is similar to DiffServ. In SCORE, core routers do not evolve per flow management. Only edge routers will take part in the per flow management process.

3.2.8 MPLS support for Differentiated Services

MPLS support for Differentiated Services has been addressed in [RFC3270]. In a Diff-Serv domain, that concept/class that ensures that all the IP packets that are forwarded based on the same Per-Hop Behavior is denoted as Behavior Aggregate. This solution allows the MPLS network administrator to make multiple Behavior Aggregates to be mapped onto LSPs. At the ingress LER of the MPLS/Diff-Serv domain, the packets are classified and marked with a DS codepoint (DSCP). The DSCP is utilized to select the Per-Hop Behavior. According to the Per-Hop Behavior, this solution can forward the traffic along the LSP. This solution is based on two types of LSPs: LSPs that transport multiple Ordered Aggregates and LSPs that transport a single Ordered Aggregate.

3.2.9 Next Steps in Signaling (NSIS)

The Next Steps in Signaling (NSIS) Working Group within IETF develops a Next Steps in Signaling (NSIS) protocol suite used to signal information about a data flow along its path in the network. The NSIS suite of protocols is envisioned to support various signaling applications that need to install and/or manipulate such state in the network.

The overall signaling protocol suite is decomposed into a generic (lower) layer, with separate upper layers for each specific signaling application. The generic lower layer is the NSIS Transport Layer Protocol (NTLP) and is specified in [RFC5971]. NTLP uses

existing transport and security protocols under a common messaging layer, the General Internet Signaling Transport (GIST). GIST is used to manage its own internal state and the configuration of the underlying transport and security protocols to ensure the transfer of signaling messages on behalf of signaling applications in both directions along the flow path. The signaling application protocol used for the support of Quality of Service (QoS) is denoted as NSIS Signaling Layer Protocol (NSLP) for Quality-of-Service Signaling (QOS-NSLP) [RFC5974].

3.2.10 Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Version 2 (MLDv2)

Internet Group Management Protocol (IGMP) is a protocol that is used by IPv4 systems to report their IP Multicast group memberships to the multicast routers [RFC2236], [RFC3376]. IGMP message is encapsulated in IPv4 datagram and the IP protocol number is 2. It is designed for establishing and maintaining multicast membership between IP host and multicast routers. IGMP provides four basic functions for IP multicast networks: (1) Join: An IGMP host indicates that it wants to become a member of a multicast group. (2) Leave: An IGMP host indicates that it doesn't want to receive any information from a multicast group. (3) Query: An IGMP router can ask the hosts which groups they belong to. (4) Membership Report: An IGMP host tells the IGMP host what groups it belongs to. Multicast Listener Discovery (MLD) is a protocol used by IPv6 routers to discover the multicast listeners on their directly attached links [RFC2710], [RFC3810].
MLD version 1 [RFC2710] operates in a similar way as the IGMP version 2 [RFC2236] in an IPv4 environment, Moreover, MLD version 2 [RFC3810] operates in an IPv6 environment in a similar way as the IGMP version 3 [RFC3376] in an IPv4 environment.

3.2.11 IGMP/MLD Based Multicast Forwarding

The IGMP/MLD multicast forwarding mechanism [RFC4605] is able to apply a spanning tree multicast routing [Deer91] to environments that are able to support IGMP and MLD protocols. The IGMP/MLD based multicast forwarding only works when a simple tree topology is deployed. The tree contains the proxy devices, such as the Local Mobility Anchor and Mobile Access Gateway whose interfaces are manually configured, see Section 3.3.2. The tree is connected to a wide multicast infrastructure. If more complicated scenarios are required where the topology is not a simple tree or where more than one domain are used, then dynamic multicast routing protocols are required.

3.2.12 Distance Vector Multicast Routing Protocol (DVMRP)

Distance Vector Multicast Routing Protocol (DVMRP) [RFC1075] is an interior gateway protocol that is used within one autonomous system. However, it is not used between different autonomous systems. DVMRP implements internetwork multicasting. DVMRP is developed for use in routing multicast data packets, but it could be extended to route

unicast data packets. DVMRP is developed based on the Routing Information Protocol (RIP) [RFC1058] and uses IGMP to exchange routing datagrams. DVMRP datagram consists of two parts: one fixed length IGMP header and a stream of tagged data.

3.2.13 Multicast Open Shortest Path First (MOSPF)

Multicast Open Shortest Path First (MOSPF) [RFC1585] is an extension to Open Shortest Path First v2 (OSPFv2) [RFC1583] to support multicast routing. It allows the user to share information about the group membership. MOSPF was implemented by several vendors and has seen some deployment in intra-domain networks. But MOSPF does not work in the inter-domain case, because it is based on the intra-domain OSPF. Due to this reason, the protocol has not been deployed by many operators.

3.2.14 Protocol Independent Multicast-Sparse Mode (PIM-SM)

Protocol Independent Multicast-Sparse Mode (PIM-SM) [RFC4601] is a protocol used to efficiently route multicast groups. Since it is not dependent on any particular unicast routing protocol, it is named protocol independent. It is suitable for the case where the density of group members belong to the same multicast session is very low. It generates a unidirectional tree structure starting from each sender to all the receivers in the multicast group.

3.2.15 Protocol Independent Multicast-Dense Mode (PIM-DM)

Protocol Independent Multicast-Dense Mode (PIM-DM) [RFC3973] is a protocol for constructing a tree for sending packets to multiple users. PIM-DM assumes that when a source wants to send multicast data, then all downstream systems are willing to receive this multicast data. Initially, the multicast data is sent to everywhere. The Reverse Path Forwarding mode is then utilized to avoid looping of multicast data. Prune messages are used when some parts of the network are not involved in the group that receives the multicast data.

3.3 IP Mobility

This section describes a number of solutions that can be used to support IP based mobility management.

3.3.1 Mobile IP

Mobile IPv4 [RFC3344] and Mobile IPv6 [RFC3775] allow a mobile node to move from one sub-network to another sub-network without changing the mobile node's home address. In Mobile IP, every node has its home address, and when the node is moving to a foreign network, it gets Care-of address (CoA) to indicate its current location. The

association between the home address and Care-of address is called binding. The mobile node sends among others the CoA to its Home Agent to do the binding. The Home Agent is the entity that is typically located in the home domain of a mobile node and is able to manage the mobility of a mobile node. When the binding is done, the home agent sends the packets to the mobile node via a tunnel that is typically established between the Home Agent and the mobile node in case of Mobile IPv6 and the Foreign Agent (FA) in case of Mobile IPv4, which is an entity that provides wireless access to the mobile node. A mobile node registers with a Foreign Agent at its current location. When the mobile node moves to different networks, it sends binding updates with its new CoA.

3.3.2 Proxy Mobile IP

Proxy Mobile IPv6 [RFC5213] and Proxy Mobile IPv4 [RFC5844] are possible ways of supporting IP based mobility management, where the participation of a mobile node in any mobility related signaling is not required.

Proxy mobile IP is designed for supporting network-based IP mobility management to a mobile node. The mobile node does not need to perform the exchanging of signaling message between the node itself and the home agent. Instead, a proxy mobility agent in the network performs the signaling task and takes care of the mobility management. There are two main entities used in Proxy Mobile IP are the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). LMA is operating as a home agent and is responsible for maintaining the topological anchor point for MNs network prefixes and the MNs reachability state. The MAG performs mobility management on behalf on the MN and it is located on the same access link where the MN is anchored. Moreover, the MAG is responsible for detecting the movements of a MN to and from the access link and when needed initiate binding registrations towards the LMA. It is important to emphasize that more than one LMA could be used in a Proxy Mobile IPv6 domain, each of them serving a different group of MNs. In this M.Sc. assignment we assume that only one LMA is used within the Proxy Mobile IP based core network.

During their communications, the MN only uses its home address (HA). The Care of Address (CoA) is only visible to its associated MAG and LMA.

A Proxy Mobile handover consists of the following steps:

(1) Handoff at the data link layer:
When MN joins the new MAG's domain, it will receive a router advertisement (Rtr Adv) message from the new MAG. From the Rtr Adv message, the MN could obtain the same prefixes of the previous MAG.

(2) Proxy Binding Update:
The previous MAG (PMAG) will send a Proxy Binding Update (PBU) message to LMA to announce that the MN will perform the handover soon. So the PMAG will need to deregister the binding registration between the Proxy-CoA of the PMAG and the HA of the MN.

(3) Proxy Binding Acknowledgement (PBA)
LMA will then send a Proxy Binding Acknowledgement (PBA) message to the PMAG to indicate that Proxy Binding Update (PBU) message is processed successfully.

(4) The new MAG (NMAG) will send a Proxy Binding Registration (PBR) message to the LMA so that the binding registration between the home network prefixes of mobile node and proxy-CoA of the NMAG can be performed.

(5) LMA will send a PBA to the NMAG to indicate that the PBU is processed successfully.

(6) Bidirectional tunnel, see [RFC3473] is set up. The MN can use the home network prefixes to attach to the MAG.

(7) MN will send a Router Solicitation (Rtr Sol) message to the NMAG.

(8) After receiving the Rtr Sol message, the NMAG will send a Router Advertisement message to the MN. This message contains the home network prefix of the mobile node. This home network prefix will be the link prefix.

After this step the link between the MN and NMAG is established and the inter-system handover is done.

3.3.3 Network Mobility (NEMO)

Network Mobility (NEMO) provides extensions to Mobile IP in order to enable an entire mobile network, e.g., a train, a plain, to attach to different points in the Internet. [RFC3963] specifies the NEMO extensions associated with Mobile IPv6 and [RFC5177] specifies the NEMO extensions associated with Mobile IPv4. NEMO allows session continuity for every node in the mobile network. In NEMO, a Mobile Router (MR) plays the role of the MN to perform mobility functions. Mobile nodes that are connected to a MR are not involved in any mobility signaling functionality. MRs are considered to be specific gateways that are able to send binding requests to their home agents. Moreover, a bi-directional tunnel between the mobile router and its home agent can be established that can be used during the data communication phase.

3.3.4 Multicast Listeners in PMIPv6

Currently, the IETF working group Multicast Mobility (multimob) [multimob] is trying to extend Proxy Mobile IP to support multicast communication. This is still work in progress. One possible approach is based on the Multicast Listener Discovery (MLD). This approach is referred as Base Deployment for Multicast Listener Support in PMIPv6 Domains [ScWa10]. It describes how to deploy multicast functions in Proxy Mobile IPv6 domains. In particular, in this solution, the Proxy Mobile IPv6 (PMIPv6) based LMA

serve as multicast subscription anchor point; while the PMIPv6 based MAG provides MLD proxy functions. An overview of this deployment is depicted in Figure 16.

Since this deployment relies on the functionalities of the network entities that are specified in PMIPv6, the operations of these entities that generally require multicast functions will be discussed below. Typically, the multicast activation in a PMIPv6 domain requires multicast functions to be deployed at routers.

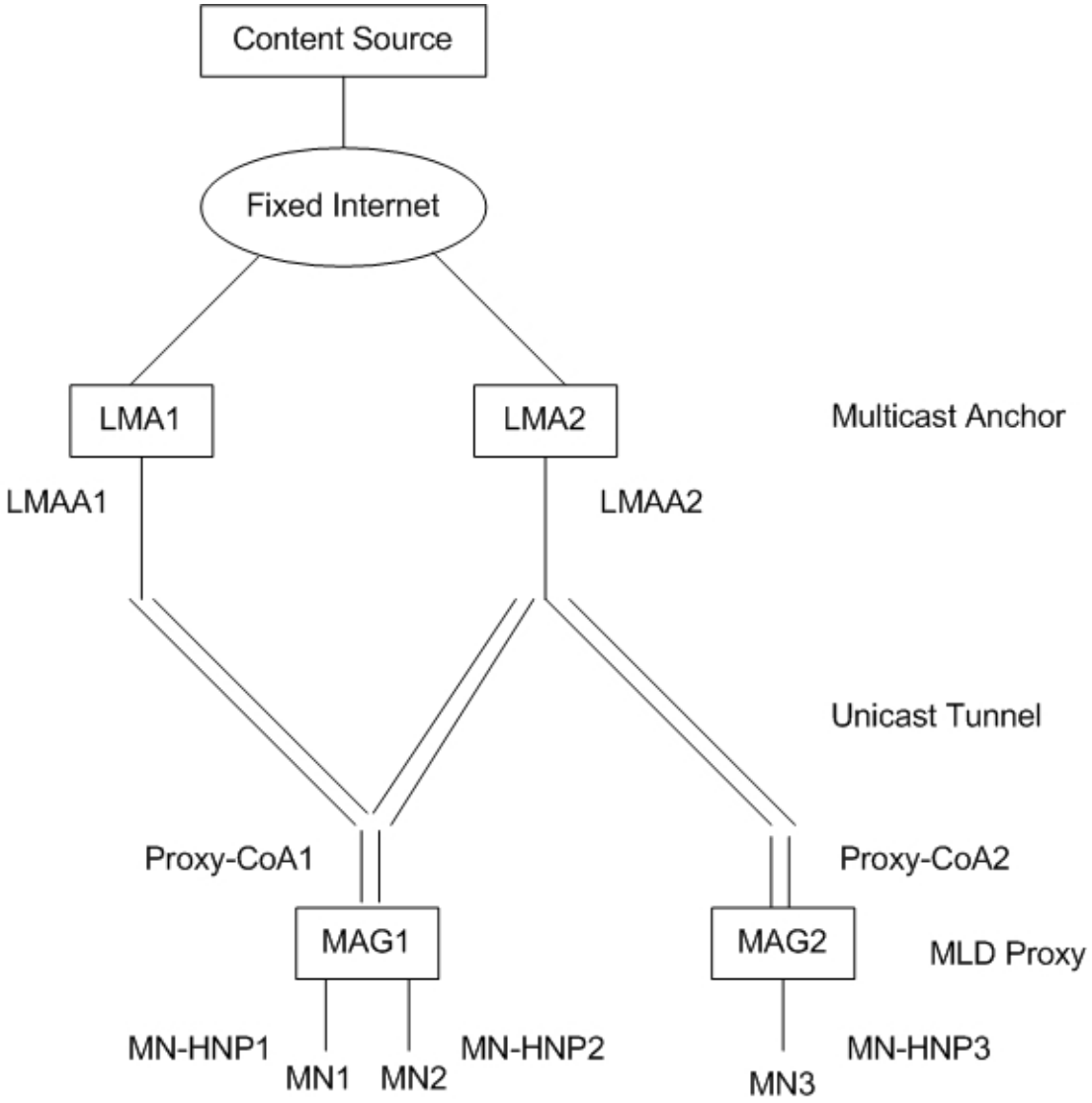

Figure 16: Overview of Multicast Deployment in PMIPv6

A Mobile Node (MN) can decide to join a multicast group regardless of its mobility status. The MN will submit a MLD report and MLD done messages using link-local source address and multicast destination addresses. These signaling messages will arrive at the MAG through one of its downstream local links. To achieve multicast in PMIPv6 domain, a MLD proxy function is deployed on the MAG so that the tunnel interface

corresponding to the MN's LMA for its upstream interface is chosen. Every MAG-to-LMA tunnel interface defines a MLD proxy domain at the MAG. Within the MLD proxy domain there are some downstream links to MNs that are initiated by this LMA, see Figure 16. LMA plays a role as either a multicast router or an additional MLD proxy. The LMA will transmit all the MLD messages from a MAG into a multicast routing domain. The multicast forwarding states at the tunnel interface are generated. Traffic that is intended to go to the groups will first go the LMA. After that, LMA will forward this traffic based on the group or source states.

MLD queries and multicast data will arrive at the tunnel interface at the MAG. The interface is linked to a group of MNs based on the access links that are identified using its Binding Update list. MAG will send the multicast traffic and the relevant signaling message along the access links to the MNs. So all the multicast data and the relevant signaling messages will be sent to the MN.

3.4 MPLS Security

The security framework that can be applied in MPLS and GMPLS is specified in [RFC5920]. This framework describes the security threats, the related defensive techniques, and the mechanisms for detection and reporting. In particular, RSVP-TE security considerations, are described, as well as inter-AS and inter-provider security considerations required to build and maintain MPLS and GMPLS networks across different domains or different Service Providers.
Regarding the security support of the PMIPv6 signaling messages, Proxy Binding Update (PBU) and Proxy Binding Acknowledgement (PBA) that are transported between the MAG and LMA (see [RFC5213] and [RFC5844]) the IPSec [RFC2401] security solutions are used. IPSec is a protocol suite for securing IP communications by authenticating and encrypting each IP packet for a communication session. IP Encapsulating Security Payload can be implemented in two modes: transport mode and tunnel mode. IPSec Encapsulating Security Payload in transport mode with mandatory integrity protection should be used for protecting the signaling messages, while confidentiality protection of these signaling messages is not necessary [RFC5213]. IPSec ESP in tunnel mode could be used for the data traffic that is transported in the tunnel when it is necessary.

Chapter 4: Specification and design of architecture for IP based interconnection of heterogeneous communication systems for mission-critical group oriented communications

This chapter describes the specification and design of the core network architecture for IP based interconnection of heterogeneous communication systems.

Figure 17 shows the proposed core network architecture for the IP based interconnection of heterogeneous communication systems. The main functionality of the core network architecture is to interconnect various heterogeneous wireless access communication systems, e.g., TETRA, WiMAX, UMTS and LTE.
Based on the state of the art presented in Chapter 3 it can be deduced that the core network architecture requirements discussed in Chapter 2 can be satisfied by using the following solutions, see also Chapter 3. For the support of the strict QoS and preemption requirements in combination with the requirement on supporting different communication modes, it is recommended that MPLS in combination with RSVP-TE for point to multipoint and MPLS multicast label are used. For the support of the mobility requirements the generic PMIP with multicast support is recommended. For the support of the security, it is recommended that IPSec in combination with the security solutions applied for MPLS are used.

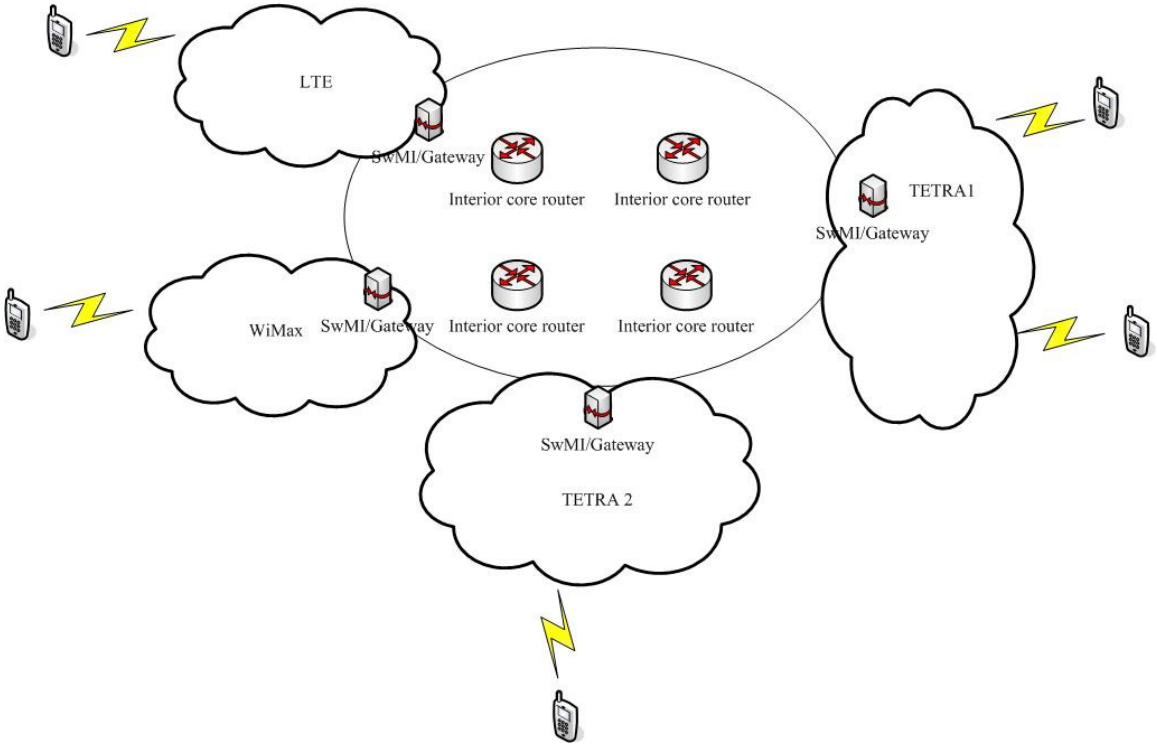

Figure 17: The architecture for IP based interconnection of heterogeneous communication systems

4.1 Functionality of the proposed architecture

4.1.1 Overview of the architecture

To describe the functionalities of our architecture, we briefly discuss the protocol stacks used at the mobile station and base station, which are given in [ETSI-EN-300392-1]. In subsequent sections the functionalities supported by the gateways and interior routers are described in more detail.

Figure 17 depicts the main entities that are used within the core network architecture. The nodes within the core network architecture are depicted as interior routers. These nodes are MPLS Label Switching Routers (LSRs). The nodes located on the boundaries of the core network architecture are edge nodes that are able to support a variety of functions. First of all they are MPLS Label Edge Routers (LER). Moreover, they are able to support TETRA SwMI functionalities.

4.1.2 Description of the functionalities of each network entity

In our architecture, some network entities are presented. Each entity performs certain functionalities. All these functionalities should be supported in order to ensure our group communication.

Gateway is a network entity for interfacing and interconnecting the MPLS IPv6 core network with one or more access networks. It needs to support the following functionalities:

- MPLS Label Edge Routers, see [RFC3031];
- Support of point-to-multipoint LSPs, see [RFC4875], [RFC5332];
- RSVP-TE for point-to-multipoint LSPs, see [RFC3209], [RFC4875], [RFC3270];
- LMA or a MAG, see [RFC5213], [RFC5844], [ScWa10];
- TETRA SwMI, which can be either a CSwMI or another SwMI type, e.g., originating, participating, see [ETSI-EN-300392-3-3];
- Data link support [ETSI-ETS-300392-4-1].

Interior core router supports the following functionalities:

- MPLS Label Switched Router (LSR), see [RFC3031];
- Support of point-to-multipoint LSPs [RFC4875], [RFC5332];
- RSVP-TE for Point-to-multipoint LSPs [RFC4875];
- Data link support: IPv6 core network, e.g. Ethernet [RFC5332].

4.2 Protocol Stack Description

The protocol stack used in the proposed core network architecture is based on the TETRA protocol stack and is enhanced by adding the additional protocol layers and an

interworking feature that is able to provide interoperability between some TETRA protocol layers and the new (added) protocol layers.

4.2.1 Protocol Stack of Gateway

The Gateway entity uses a protocol stack that consists of two parts: control plane and user plane. The control plane comprises the protocols that are used for signaling, while the user plane comprises the protocols that are used for user data transport, such as video, telephony, streaming, best effort user data.
Since the Gateways are located between the core network and the wireless access networks the protocol stack (both control plane and user plane) can be divided in two parts. One part is used for the communication with the core network entities and the other part is used by the Gateway to communicate with the entities located in wireless access networks (e.g., TETRA).

4.2.1.1 Control Plane of Gateway Protocol Stack

The Gateway protocol stack used for the control plane is shown in Figure 18. The left part of this protocol stack represents the protocol layers for the communication with the core network entities, while the right part represents the protocol layers used to communicate with the entities located in the wireless access networks (TETRA).

The control plane protocol layers used by the Gateway to communicate with the core network entities are:

- Physical and data link layers based on wired technologies such as Ethernet [MeBo76], SONET [SiSh96], SDH [SiSh96];
- MPLS protocol suite, see Chapter 3, comprising also the Security framework for MPLS and GMPLS [RFC5920];
- Network layer based on IPv6 [RFC2460] (or IPv4 [RFC791]) comprising group management protocols, such as IGMP or MLD membership information [RFC5186], [[RFC 4605], and routing protocols such as DVMRP [RFC1075], MOSPF [RFC1585], PIM-SM [RFC4601], PIM-DM [RFC3973];
- UDP transport protocol [RFC768];
- RSVP-TE for point-to-multipoint, [RFC3209], [RFC4875], [RFC3270], [RFC5332];
- PMIP [RFC5844], [RFC5213], PMIP with multicast [RFC5757], [ScWa10];
- IPSec [RFC4301].

The right part of the protocol stack comprises the protocol layers that are used by a Gateway to communicate with entities that are located in the wireless access network (TETRA). These protocol layers are:

- The physical and data link layers used by the wireless access technology. In this assignment it is considered that the used wireless access technology is TETRA.

Therefore, it is considered that these layers are TETRA layers [ETSI-EN-300392-2];

- The network layer used by the wireless technology (TETRA). These are the Mobile Link Control Entity, Sub-Network Dependent Control Protocol (SNDCP) Packet Handling, Circuit Mode Control Entity, Mobility Management [ETSI-EN-300392-1] [ETSI-EN-300392-2].

Figure 18 depicts a feature that is denoted as Interworking function. This function performs the functionality that is needed by the Gateway in order to be able to interwork and exchange signaling messages between the left and right parts of the protocol stack depicted in Figure 18. In particular, the interworking function defines how and when protocol layers such as MPLS, IP, RSVP-TE, and PMIP with multicast support interoperate with the TETRA based protocols shown in the right part of Figure 18.
This interworking and interoperation between the left and right parts of the protocol stack given in Figure 18 is specified using the message sequence charts that are described in Section 4.3.

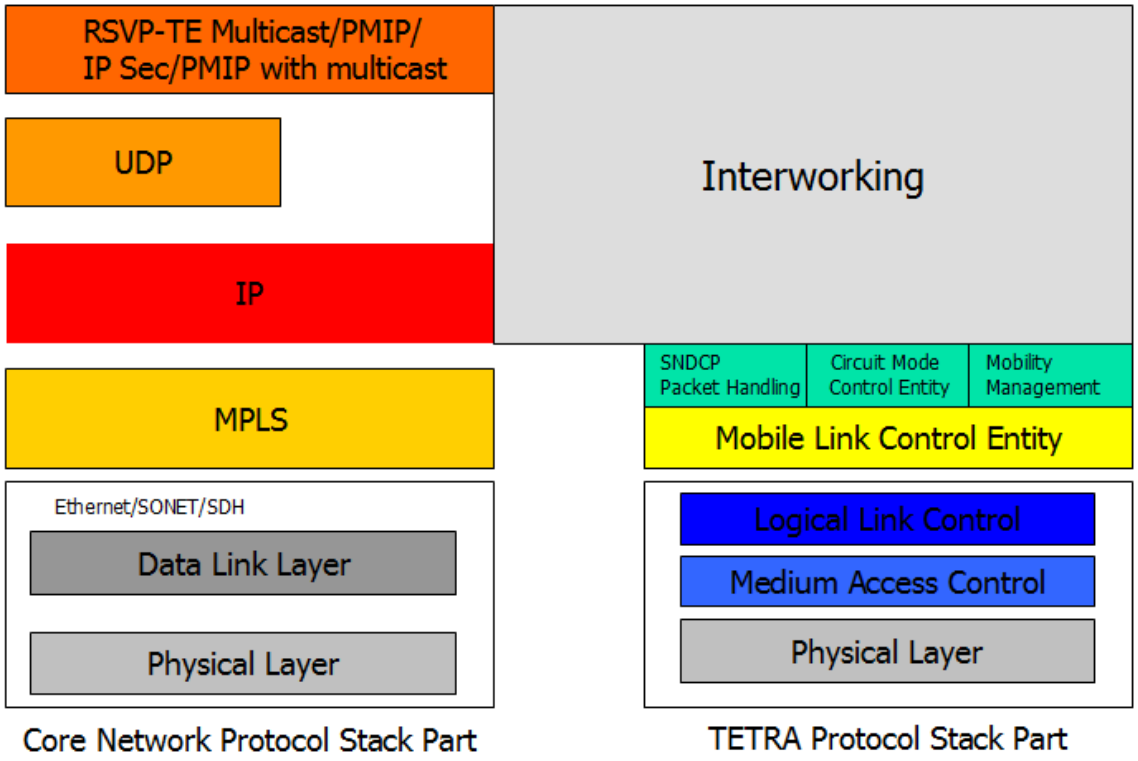

Figure 18: Control plane of Gateway Protocol stack

4.2.1.2 User Plane of Gateway Protocol Stack

The user plane of the gateway protocol stack is shown in Figure 19. The user plane handles the user data transport.

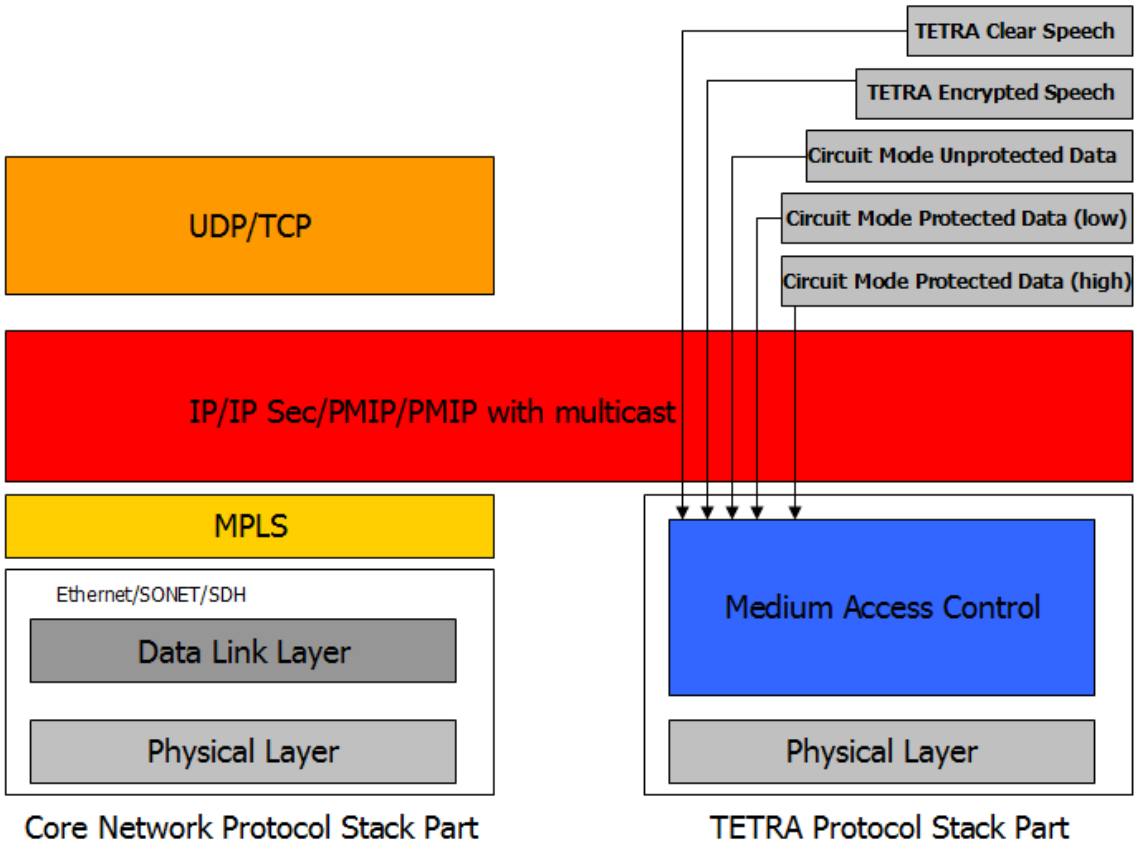

Figure 19: User plane of Gateway Protocol stack

The user plane protocol layers used by the Gateway to communicate with the core network entities are:

- Physical and data link layers based on wired technologies such as Ethernet [MeBo76], SONET [SiSh96], SDH [SiSh96];
- MPLS protocol suite, see Chapter 3, comprising also the Security framework for MPLS and GMPLS [RFC5920];
- Network layer based on IPv6 [RFC2460] (or IPv4 [RFC791]) comprising group management protocols, such as IGMP or MLD membership information [RFC5186], [[RFC 4605], and routing protocols such as DVMRP [RFC1075], MOSPF [RFC1585], PIM-SM [RFC4601], PIM-DM [RFC3973];
- UDP transport protocol [RFC768], or TCP transport protocol [RFC793];
- PMIP [RFC5844], [RFC5213], PMIP with multicast [RFC5757], [ScWa10];
- IPSec [RFC4301].

The right part of the protocol stack comprises the protocol layers that are used by a Gateway to communicate with entities that are located in the wireless access network (TETRA). These protocol layers are:

- The physical and data link layers used by the wireless access technology. In this assignment it is considered that the used wireless access technology is TETRA. Therefore, it is considered that these layers are TETRA layers [ETSI-EN-300392-2]

- The application layers used by the wireless technology (TETRA). These are protocols that are used to support TETRA speech and TETRA circuit mode data [ETSI-TR-300-1].

It is important to note that the Internet Protocol layer can be used in the user plane to provide the required interworking and interoperation between the left part and right part of the user plane protocol stack depicted in Figure 19.

4.2.1.3 Main Functionalities of Gateway

This section briefly describes the main functionalities that are supported by the Gateway. Since the gateway is located at the boundary of the wireless access network, and it needs to interconnect the core network with the wireless access network, the first functionality that is supported by the gateways is the functionality provided by a MPLS Label Edge Router (LER). This functionality has been discussed in Section 3.2.3.

Point-to-multipoint LSPs (Label Switched Paths) is a functionality that needs to be supported for multicast communication. Point-to-multipoint LSPs could be set up by RSVP-TE and the Label distribution protocol (LDP). Moreover, RSVP-TE can be used to setup multicast trees with QoS support. One critical issue is how to map the 'heterogeneous receivers' paradigm onto a link layer [RFC3353]. The fundamental approaches are the 'Limited Heterogeneity Model' and the 'Homogeneous Model'. The first approach will generate two trees. One is for a best effort service and another is meant for a single alternate QoS enabled service. The sender will send its traffic twice. The second approach only generates one QoS tree. The best-effort users are connected to the QoS tree. If the branches that are utilized for best-effort users cannot perform label switching, these QoS multicast traffic has to be merged onto the default LSPs that can carry best-effort traffic. Merging QoS multicast traffic onto the default LSPs is done by mixing the L2 and L3 forwarding. L2/L3 forwarding is performed by the nodes that can distribute a multicast tree into branches that are either forwarded at L3 or switched at L2.

In [RFC4875], a solution for duplicating data is achieved by enabling non-ingress nodes to be branch nodes that are capable of duplicating data onto outgoing interfaces. In order to do this, Point-to-multipoint (P2MP) LSP has to be set up using RSVP-TE. Thus the second functionality that needs to be supported by the gateway is the RSVP-TE for Point-to-multipoint (P2MP) LSP. P2MP LSP consists of one or multiple source to leaf sub-LSPs. It is required that add and remove endpoints to and from P2MP LSP must be possible.

Source to leaf (S2L) sub-LSPs exist within the context of a P2MP LSP. S2L sub-LSP is identified by the P2MP ID, Tunnel ID, extended Tunnel ID, the tunnel sender address, LSP ID fields of the P2MP sender_TEMPLATE object and the S2L sub-LSP destination address. The first three IDs are part of P2MP session while S2L sub-LSP destination address is part of the S2L_SUB_LSP object.

An individual P2MP LSP can be signaled by means of one or multiple Path messages. Each Path message can signal one or more sub-LSPs. Multiple Path messages can be supported since one path message may not contain all the S2L sub-LSPs due to the limitation of its size.

MPLS offers two options for selecting routing paths, namely: hop by hop routing and explicit routing. In explicit routing, LSP uses the communication path that is defined by the ingress node. Explicit Route Object (ERO) or P2MP_Secondary_Explicit_Route Object (SERO) is used to specify the explicit route of a S2L sub_LSP. Each ERO or SERO that is signaled corresponds to a particular S2L_SUB_LSP object. A Path message could signal a single S2L sub-LSP or multiple S2L sub-LSPs. When a single S2L sub-LSP is signaled, the Path message is sent only to the leaf of the P2MP tree. < Explicit_Route > together with <S2L_SUB_LSP> are the representations of the S2L sub-LSPs. If the ERO is not included in the Path message, it means that hop-by-hop routing is required.

A Path message could also signal multiple S2L sub-LSPs, the path of the first S2L to the egress LSR is encoded in the ERO. The first S2L sub-LSP will correspond to the first S2L_SUB_LSP object that is present in the Path message. Other S2L sub-LSPs will be formed in sequence. SERO contains information concerning every S2L_SUB_LSP, which can form the whole P2MP LSP. In order to keep the path information as little as possible, all the repetition of the path information that is produced by S2L_SUB_LSP with the same hops is decreased by means of using the explicit route compression.

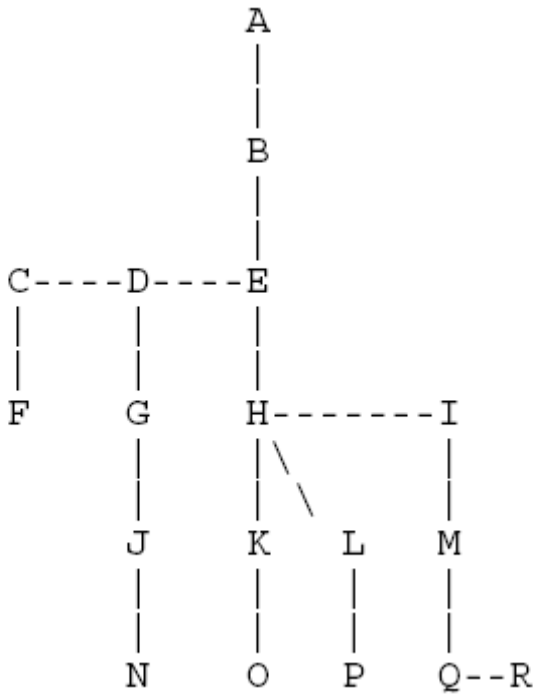

Figure 20: A P2MP LSP, from [RFC4875]

This path can be divided into several hops that are defined by the ingress LSR. Figure 20

shows a P2MP LSP with LSR A as the ingress LSR and six egress LSRs: (F, N, O, P, Q and R). When all six S2L sub-LSPs are signaled in one Path message, we assume that the S2L sub-LSP to LSR F is the first S2L sub-LSP. The remaining sub-LSPs are subsequent S2L sub-LSPs. The ingress LSR A encodes the S2L sub-LSP explicit routes based on the compression:

S2L sub-LSP-F: ERO= {B, E, C, D, F}, <S2L_SUB_LSP> object F
S2L sub-LSP-N: SERO= {D, G, J, N}, <S2L_SUB_LSP> object N
S2L sub-LSP-O: ERO= {E, H, K, O}, <S2L_SUB_LSP> object O
S2L sub-LSP-P: ERO= {H, L, P}, <S2L_SUB_LSP> object P
S2L sub-LSP-Q: ERO= {H, I, M, Q}, <S2L_SUB_LSP> object Q
S2L sub-LSP-R: ERO= {Q, R}, <S2L_SUB_LSP> object R

The essential idea of using explicit routing is that the hops that are shared by the S2L sub-LSPs will emerge only once.

Proxy mobile IP with multicast is addressed by the Internet draft Base Deployment for Multicast Listener Support in PMIPv6 Domains [ScWa10]. Readers are recommended to refer to Section 3.3.4.

4.2.2 Protocol Stack of Interior Core Router

Similar to the Gateway entity, the Interior core router uses a protocol stack that consists of two parts: control plane and user plane. The control plane comprises the protocols that are used for signaling, while the user plane comprises the protocols that are used for user data transport, such as video, telephony, streaming, best effort user data.

4.2.2.1 Control Plane of Interior Core Router Protocol Stack

The control plane protocol stack of interior core router is shown in Figure 21.
The control plane protocol layers used by the interior core router are:

- Physical and data link layers based on wired technologies such as Ethernet MeBo76], SONET [SiSh96], SDH [SiSh96];
- MPLS protocol suite, see Chapter 3, comprising also the Security framework for MPLS and GMPLS [RFC5920];
- Network layer based on IPv6 [RFC2460] (or IPv4 [RFC791]) comprising routing protocols such as DVMRP [RFC1075], MOSPF [RFC1585], PIM-SM [RFC4601], PIM-DM [RFC3973];
- UDP transport protocol [RFC768];
- RSVP-TE for point-to-multipoint, [RFC3209], [RFC4875], [RFC3270], [RFC5332];
- IPSec [RFC4301].

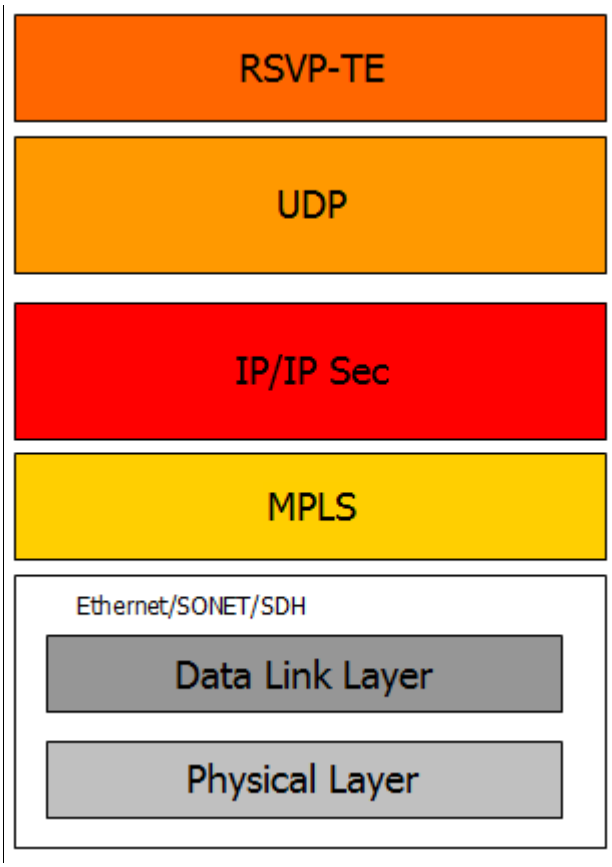

Figure 21: Control Plane of Interior Core Router Protocol Stack

4.2.2.2 User Plane of Interior Core Router Protocol Stack

User Plane of Interior Core Router Protocol Stack handles the user data transport for the interior core router. The user plane protocol stack used by an interior core router is shown in Figure 22. The user plane protocol layers used by the interior core router to communicate with the core network entities are:

- Physical and data link layers based on wired technologies such as Ethernet [MeBo76], SONET (Synchronous Optical Networking)[SiSh96], SDH [SiSh96];
- MPLS protocol suite, see Chapter 3, comprising also the Security framework for MPLS and GMPLS [RFC5920];
- Network layer based on IPv6 [RFC2460] (or IPv4 [RFC791]) comprising routing protocols such as DVMRP [RFC1075], MOSPF [RFC1585], PIM-SM [RFC4601], PIM-DM [RFC3973];
- UDP (User Datagram Protocol) transport protocol [RFC768], or TCP (Transmission Control Protocol) transport protocol [RFC793];

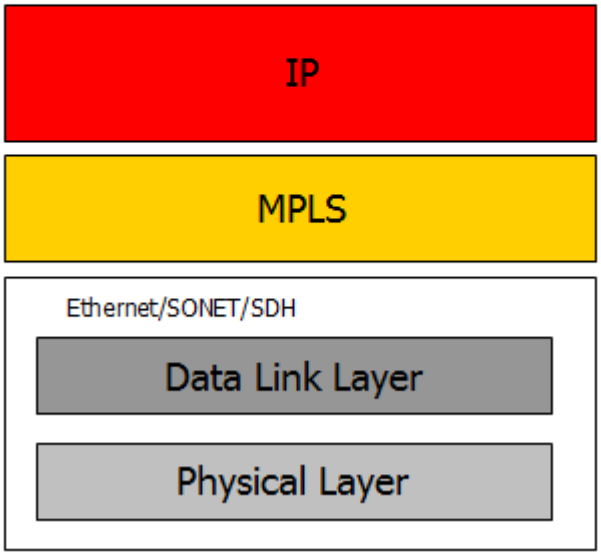

Figure 22: User plane of Interior Core Router Protocol Stack

4.2.2.3 Main Functionalities of Interior Core Router

Interior core routers should support the functionality of Label Switching Router (LSR), see Chapter 3. An LSR is a router that is able to support the MPLS protocol suite. As a packet of a connectionless network layer protocol travels from one router to the next, each router makes an independent forwarding decision for that packet. That is, each router analyzes the packet's header, and each router runs a network layer routing algorithm. Each router independently chooses a next hop for the packet, based on its analysis of the packet's header and the results of running the routing algorithm.

Packet headers contain considerably more information than is needed simply to choose the next hop. Choosing the next hop can therefore be thought of as the composition of two functions. The first function partitions the entire set of possible packets into a set of "Forwarding Equivalence Classes (FECs)". The second maps each FEC to a next hop. Insofar as the forwarding decision is concerned, different packets which get mapped into the same FEC are indistinguishable. All packets which belong to a particular FEC and which travel from a particular node will follow the same path (or if certain kinds of multi-path routing are in use, they will all follow one of a set of paths associated with the FEC).

In conventional IP forwarding, a particular router will typically consider two packets to be in the same FEC if there is some address prefix X in that router's routing tables such that X is the "longest match" for each packet's destination address. As the packet traverses the network, each hop in turn reexamines the packet and assigns it to a FEC.

In MPLS, the assignment of a particular packet to a particular FEC is done just once, as the packet enters the network, by the ingress LER. The FEC to which the packet is assigned is encoded as a short fixed length value known as a "label". When a packet is forwarded to its next hop, the label is sent along with it; that is, the packets are "labeled" before they are forwarded.

At subsequent hops, there is no further analysis of the packet's network layer header. Rather, the label is used as an index into a table which specifies the next hop, and a new label. The old label is replaced with the new label, and the packet is forwarded to its next hop.

In the MPLS forwarding paradigm, once a packet is assigned to a FEC, no further header analysis is done by subsequent routers; all forwarding is driven by the labels. This has a number of advantages over conventional network layer forwarding.

1. MPLS forwarding can be done by switches which are capable of doing label lookup and replacement, but are either not capable of analyzing the network layer headers, or are not capable of analyzing the network layer headers at adequate speed.

2. Since a packet is assigned to a FEC when it enters the network, the ingress LER may use, in determining the assignment, any information it has about the packet, even if that information cannot be gleaned from the network layer header. For example, packets arriving on different ports may be assigned to different FECs. Conventional forwarding, on the other hand, can only consider information which travels with the packet in the packet header.

3. A packet that enters the network at a particular LER can be labeled differently than the same packet entering the network at a different router, and as a result forwarding decisions that depend on the ingress router can be easily made. This cannot be done with conventional forwarding, since the identity of a packet's ingress router does not travel with the packet.

4. The considerations that determine how a packet is assigned to a FEC can become ever more and more complicated, without any impact at all on the routers that merely forward labeled packets.

5. Sometimes it is desirable to force a packet to follow a particular route which is explicitly chosen at or before the time the packet enters the network, rather than being chosen by the normal dynamic routing algorithm as the packet travels through the network. This may be done as a matter of policy, or to support traffic engineering. In

conventional forwarding, this requires the packet to carry an encoding of its route along with it ("source routing"). In MPLS, a label can be used to represent the route, so that the identity of the explicit route need not be carried with the packet.

LSR is an MPLS node that has capability to support MPLS capabilities, including point-to-multipoint RSVP-TE features and that is able to forward layer 3 packets.

In general, an MPLS packet is transmitted via a data link, via an MPLS tunnel or an IP tunnel. For each case, when the packet is sent along the tunnel, the downstream LSR must know whether the top label in the label stack has an upstream-assigned label binding or a downstream-assigned label binding. The transmission is done in a data link layer by encapsulating the MPLS packet in a data link layer frame and transmitting the frame. The MPLS packet can also be transmitted through an MPLS tunnel or first transmitted in an IP-based tunnel and then transmitted in a data link layer and/or in an MPLS tunnel.
MPLS can be used in combination with data link layers, such as Ethernet [IEEE Ethernet]. MPLS can support different types of Label Switching Paths (LSPs), such as point-to-point LSPs [RFC3032] and point-to-multipoint LSPs [RFC5332].

The way of how point-to-multipoint LSPs are used in combination with the multipoint-to-multipoint Ethernet is specified in [RFC5332]. In particular, [RFC5332] specifies in detail how an MPLS packet can be carried in an Ethernet multicast frame, comprising the specification on how the Medium Access Layer Destination Address (MAC DA) field is to be set.

4.3 Main Message Sequence Charts supported by the Core Network Architecture

In this section, Message Sequence Charts have been derived to show the operation of the signaling protocols that have been described in previous subsections of Chapter 4.

MPLS multicast LSPs can be set up either for signalling message that needs to be sent within the core network architecture or for the user data that is transported among several wireless access networks.

To show how the core network architecture can support TETRA services, we focus on the most important service: Group call. The main steps for enabling a group call and its associated user data transport, are group establishment, (group) call setup, call maintenance (i.e., push to talk), (group) call release, (group) call handover and group leave. In the following subsections, we will define message sequence charts for the possible call acceptance and call connection modes that are among others based on the signaling diagram that are given in [ETSI-EN-300392-3-3] and extended using the signaling diagrams used by other protocols, such as RSVP-TE, PMIP with multicast support, IGMP/MLD.

It is important to note that in [ETSI-EN-300392-3-3] it is specified that there are two resource allocation policies for a PSwMI to allocate resources during the call setup and call maintenance (i.e., push-to-talk): 1. permanently allocated resources policy; 2. temporary allocated resources policy. For the permanently allocated resources policy, all resources reserved during call set-up should be available for the call maintenance. So during the call setup the resources should be reserved using RSVP-TE procedures, while during call maintenance (i.e., push-to-talk), it is not needed to reserve and allocate resources. For the temporary allocated resources policy, the resources are not allocated during the call setup, but they are temporarily allocated by the call maintenance (i.e., push to talk) signaling procedures. So, during the call maintenance the CSwMI has to use RSVP-TE procedures to temporarily assign the required resources.

4.3.1 Group Establishment

Group establishment is the first step for using group call communication. We need to create a group before a group call is set up. For the group establishment, we consider that the Group TETRA Subscriber Identity (GTSI) registration at home SwMI will be done by the network operator.

GTSI is a TETRA Subscriber Identity assigned to a group. GTSI consists of three parts: Mobile Country Code (MCC), Mobile Network Code (MNC), and Group Short Subscriber Identity (GSSI). GTSI has the size of 48 bits. The structure of GTSI is shown in the Figure 23.

Mobile Country Code (MCC)	Mobile Network Code (MNC)	Group Short Subscriber Identity (GSSI)
10 bits	14 bits	24 bits

Figure 23: The structure of GTSI

After the GTSI registration is made, a mobile node will attach to the network. Since Proxy mobile IP is used to support mobility, the home SwMI in TETRA network will play the role of a Local Mobility Anchor (LMA).

The reason for using proxy mobile IP to support mobility is that our core network is IP based, and we want to use a generic solution that is based on IP layer and that is able to support the mobility management for users that are roaming among various heterogeneous wireless access networks. Moreover, we consider that the mobile nodes (MNs), used by such roaming users, will probably not be able to support the signaling used by such mobility management procedures. Therefore, Proxy Mobile IP (PMIP) is used instead of Mobile IP.

Group establishment uses the multicast group attachment, see Figure 24. This procedure is based on the call flow of multicast-enabled PMIP from [ScWa10].

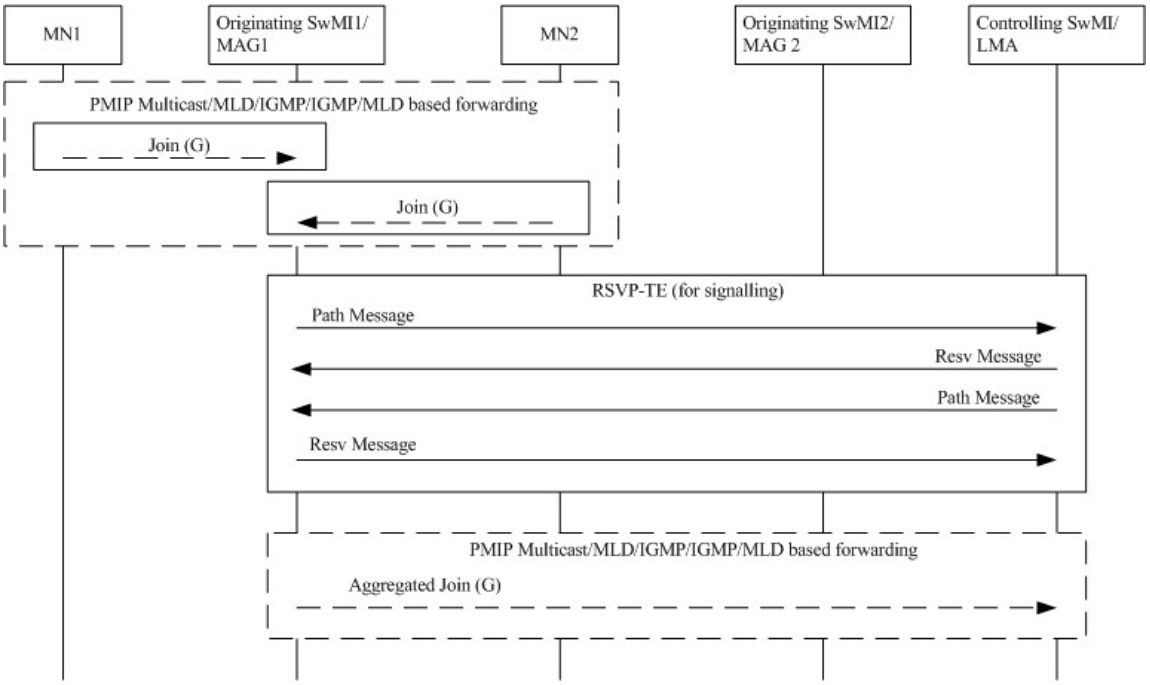

Figure 24: Group attachment

As we can see in Figure 24, the Multicast Listener Discovery (MLD) membership report that is abbreviated by the "Join" is received by the Mobile Access Gateway (MAG) in the proxy mobile IP domain.

Once receiving the MLD reports from an MN, the MAG will insert/update/remove multicast forwarding state on the incoming interface, and will put state updates into the Proxy membership database. MAG has to send an aggregated Report to the LMA. . According to [RFC4605], the proxy device enables the router function part of the IGMP/MLD protocol on each downstream interface. At each interface, the IGMP/MLD is configured, and if applicable, the highest version of IGMP/MLD applies.

The outcome of the IGMP/MLD-based multicast forwarding is a set of subscriptions and each of them is separately on each downstream interface. These subscriptions are formed into the membership database, which can be considered as a list of records with the form as:

(Multicast-address, filter-mode, source-list)

MAG will trigger the Multicast state updates and will aggregate subscriptions of all its MNs. This step is known as Aggregated Join, which will trigger the RSVP-TE procedures to reserve the path.

It is important to note that the RSVP-TE signaling procedures shown in Figure 24 set two individual point-to-point LSPs between a MAG and LMA. These point-to-point LSPs will be used within the core network by all the subsequent signaling protocols.

4.3.2 Call Setup

The second step for using group call is call setup. In this section, some scenarios used by the group call set-up signaling procedures will be illustrated. All the message sequence charts are defined based on the signaling diagram examples from [ETSI-EN-300392-3-3] and extended using the signaling diagrams used by other protocols, such as RSVP-TE.

In the subsequent Group Call establishment sections it is considered that the core network uses the permanently allocated resources policy. If the core network would use a temporary allocated resources policy, then the used RSVP-TE procedures will not apply during the call setup phase.

4.3.2.1 Single Calling Party, No Queuing for Resources

In the group communication, the simplest scenario that can be identified is the one where only one single calling party is present, and there is no need to queue for resources, see Figure 25.

Figure 25 shows the normal and most common case for call setup. The format of all TETRA messages is defined in [ETSI-EN-300392-3-3]. According to Annex E (Signaling Diagram Examples) in [ETSI-EN-300392-3-3], Mobile station one (MS1) sends a U-Setup message to the Originating SwMI. Then the originating SwMI/MAG sends the ISI-Originating Setup to the CSwMI/LMA. After that, the D-Call-Proceeding message is sent to the Mobile Station one (MS 1) as a response to the U-Setup. As we can see in the TETRA procedure box in Figure 25, after the CSwMI/LMA gets the ISI-Originating Setup, it sends ISI-Setup Initiate to all the MAGs that are present in the different TETRA domains. All the MAGs send the ISI-Setup Acknowledge to the CSwMI/LMA. After all the ISI-Setup Acknowledge messages have arrived at CSwMI/LMA, RSVP-TE is used to set up point-to-multipoint LSPs for the user data that could be transported afterwards. All these RSVP-TE procedures are based on [RFC 3209] and [RFC 4875]. Considering that there are three MAGs in this call setup scenario, each MAG sends RSVP_Path* message towards LMA. Then LMA needs to set point-to-multipoint LSPs between LMA and different MAGs. If the point-to-multipoint LSPs are successfully made, LMA can send RSVP_Resv* messages to these three MAGs. So if one MAG is the transmitter, it can use multicast communication that is arranged by these RSVP-TE procedures. Since in our core network, we have multiple interior core routers, the number of RSVP_Path messages is dependent on the number of the interior core routers located on a point-to-multipoint LSP. We use RSVP_Path* to indicate that the RSVP_Path message is transmitted within the core network. Assume that m represents the number of the interior core routers that can be located on one point-to-multipoint LSP between the LMA and two or more MAGs, then the RSVP_Path* message will be consisted of (m+1) RAVP Path messages. Note that the value of m is difficult to be defined in a deterministic way. This is because this will depend on the multicast routing manner used and on the location of the destination MAGs.

Note that in order to make point-to-multipoint LSPs that are used to support a bidirectional communication between the LMA and MAGs, the MAGs also need to start a RSVP-TE procedure towards the LMA.

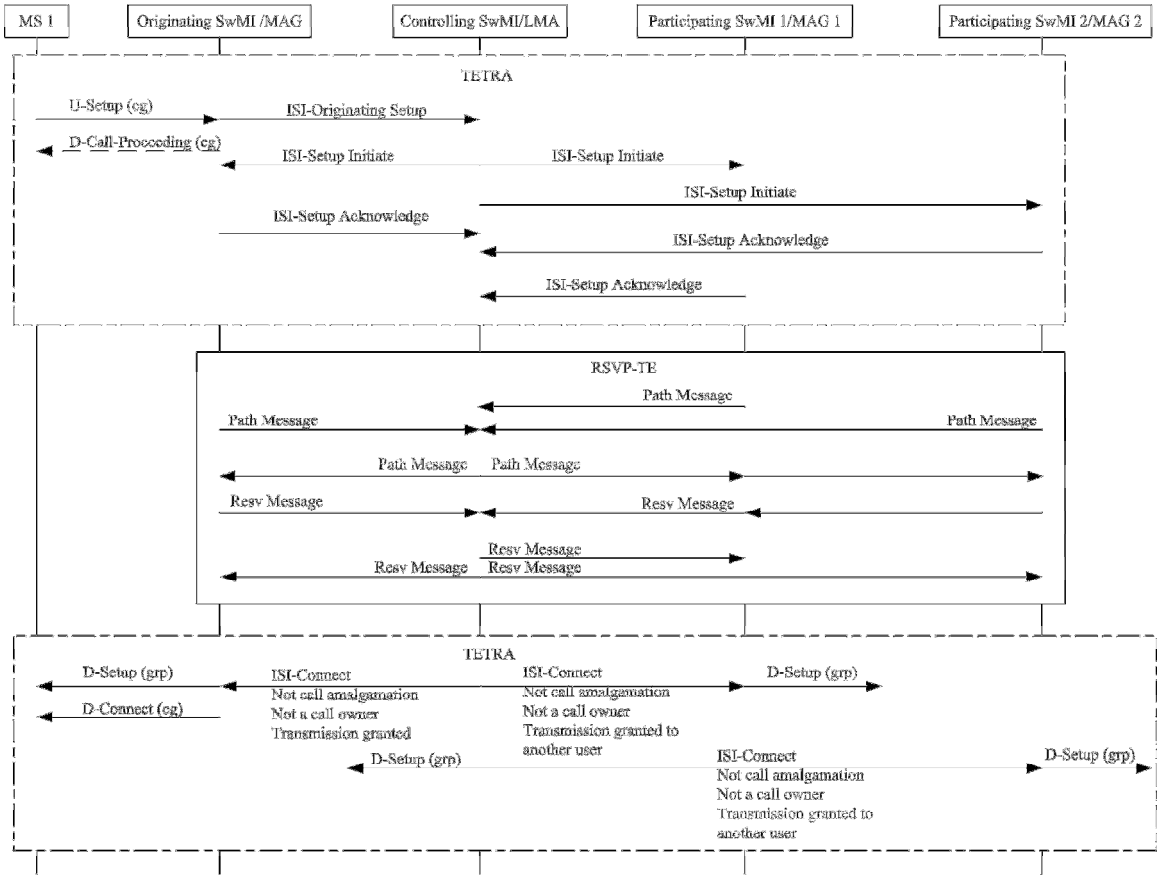

Figure 25: Successful group call set-up: single calling party, no queuing for resources

If the resources have been allocated successfully, by the RSVP-TE signaling procedures, then the second TETRA procedure box applies. In the second TETRA procedure box, ISI-Connect messages are used to connect Originating SwMI, PSwMI1 and PSwMI2. Then the downlink setup messages (D-Setup) are transmitted by the Originating SwMI, PSwMI1 and PSwMI2 to the group members, and downlink connect message (D-Connect) is sent to the MS1 so that all the group members are joining the group call.
This will cause that the point-to-multipoint LSPs are made for transporting the user data using a bi-directional communication mode.

However, if the RSVP-TE procedures could not reserve the required network resources successfully due to unavailable core network resources, or due to the fact that an error happens in the CSwMI/LMA, a different type of Message Sequence Chart has to be used, see Figure 26.

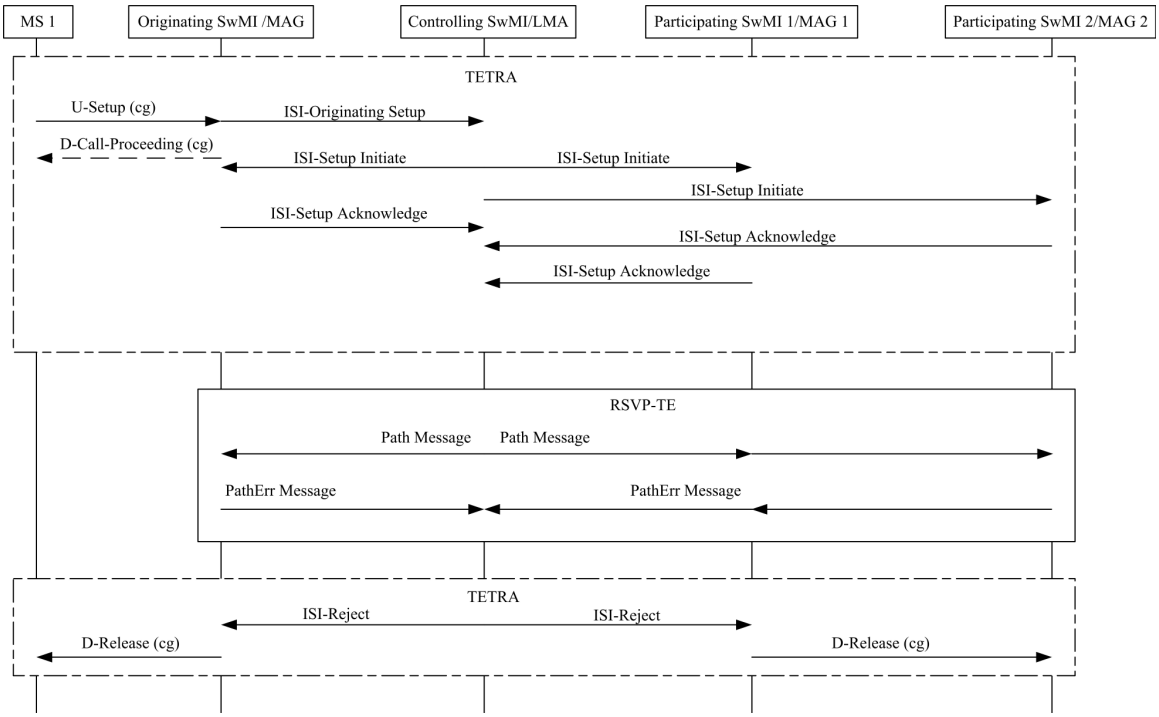

Figure 26: Unsuccessful group call set-up: single calling party, no queuing for resources

The main difference between the successful group call set-up and the unsuccessful group call set-up, see Figure 26, is associated with the RSVP-TE procedure box and the second TETRA procedure box. Since the RSVP_Path* message cannot be satisfied by the core network, the Originating SwMI/MAG has to send a PathErr* message back to the CSwMI/LMA. These RSVP-TE procedures are based on [RFC3209], [RFC4875]. In this way, the CSwMI/LMA will be notified that the resources cannot be allocated so it will send the ISI-Reject message to both the OSwMI and PSwMI1. Afterwards, the OSwMI and PSwMI1 will send downlink release messages to the calling group to release the group. The second TETRA signaling box is based on the Figure E.23 unsuccessful group call establishment from Annex E of [ETSI-EN-300392-3-3].

4.3.2.2 Single Calling Party, Some Queuing for Resources

Another scenario that can be used for call setup is the single calling party call setup, when some queuing is reserved for resources. This is shown in the Figure 27.

In the first TETRA box, the CSwMI/LMA connects the Originating SwMI/MAG and Participating SwMIs when they are ready. The MS1 sends the U-Setup to the Originating SwMI/MAG so that the Originating SwMI/MAG triggers the CSwMI/LMA to send the ISI-Setup Initiate messages to all the relevant MAGs. Then the CSwMI/LMA waits for the feedback. When all the initial responses such as the ISI-Delay and ISI-Setup Acknowledge arrive at the CSwMI/LMA, it evaluates whether the call should be delayed or partially be set up by sending either an ISI-Release or an ISI-Connect message, respectively, towards the SwMIs. If the Originating SwMI/MAG is not yet ready (it sends

ISI-delay to the CSwMI/LMA), then the CSwMI/LMA sends the ISI-Release to delay the call. After this step, the first ISI-Setup Acknowledge that arrives at the CSwMI/LMA means that another decision has to be made by the CSwMI/LMA. The CSwMI/LMA should re-evaluate whether it should try to make the call setup or continue to delay the call.

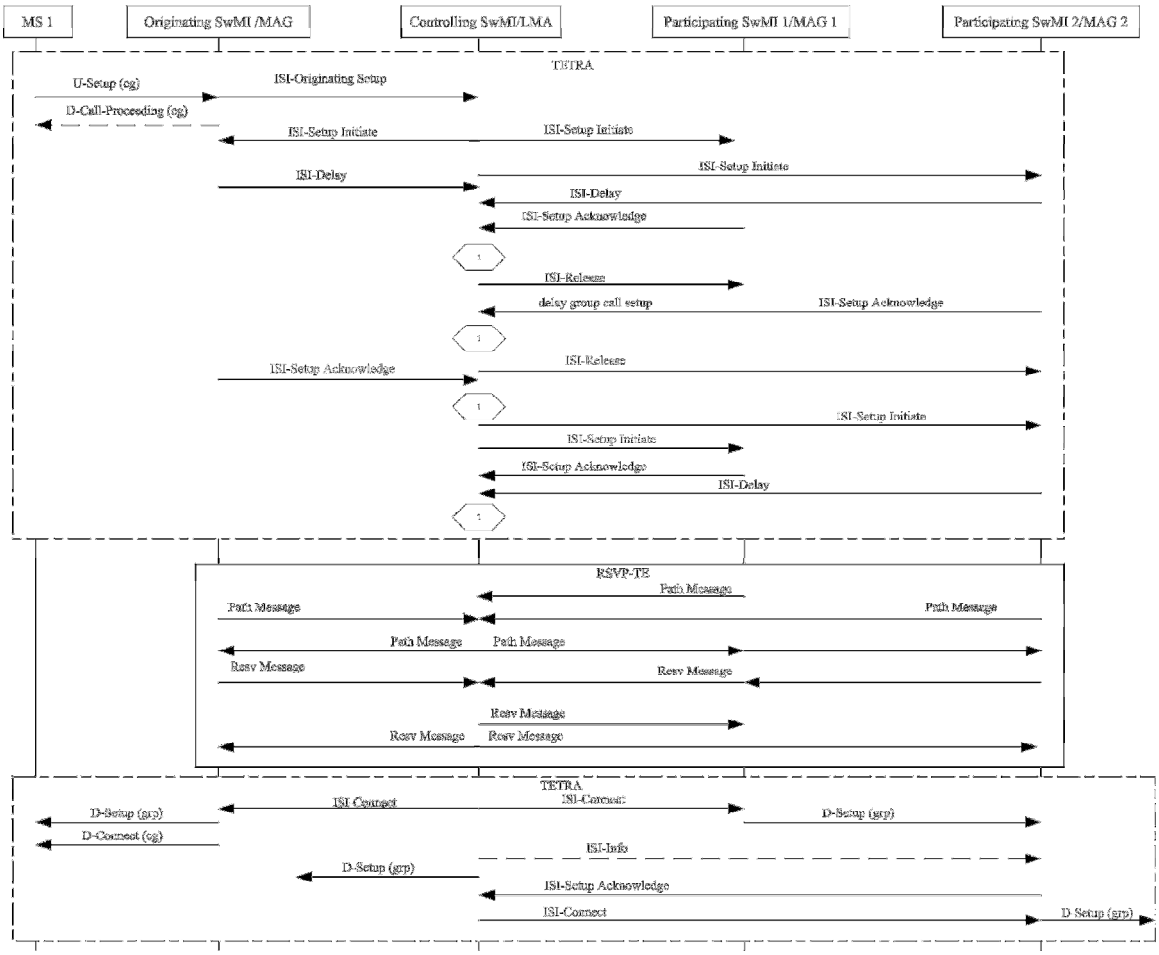

Figure 27: Successful group call set-up: single calling party, some queuing for resources

As long as CSwMI/LMA receives the ISI-Setup Acknowledge from the Originating SwMI/MAG, a new evaluation is done where it can be decided to reactivate the call. Therefore, the CSwMI/LMA sends ISI-Setup Initiate messages to all the delayed SwMIs. The last step within the first TETRA box is that another re-evaluation is conducted after all the responses to the ISI-Setup Initiate messages arrive at the CSwMI/LMA. The outcome of this re-evaluation is that both the Originating SwMI/MAG and the PSwMI1/MAG 1 are ready for the call setup while the PSwMI2/MAG 2 is not yet ready. The TETRA procedures in the first TETRA box are based on Figure E.2 given in [ETSI-EN-300392-3-3].

When all these TETRA signalling procedures are satisfied, point-to-multipoint LSPs have to be setup among the LMA and these MAGs. The RSVP-TE procedures are exactly the

same as the ones used for the successful group call setup that is given in Section 4.3.2.1. The different MAGs send RSVP_Path* message towards the LMA. Then LMA starts to make LSPs, which are between LMA and each MAG. If the point-to-multipoint LSPs have been set up successfully, LMA sends the RSVP_Resv* message back to the different MAGs. This will cause that the point-to-multipoint LSPs are made for transporting the user data using a bi-directional communication mode.

After the RSVP-TE procedures are completed successfully, the Originating SwMI/MAG and the PSwMI1/MAG 1 are connected via the CSwMI. The PSwMI2/MAG 2 is connected at last. Now different users from various MAGs are connected to the call.

4.3.2.3 Multiple Calling Parties

In this section, a successful scenario for multiple calling parties is presented. In this scenario, a new calling party is associated with the OSwMI2, see Figure 28.

At the beginning, MS1 starts to make a call setup by sending a U-Setup message to the Originating SwMI/LMA1. The Originating SwMI/LMA triggers the CSwMI/LMA to send ISI initiate signaling messages between the different SwMIs. The CSwMI/LMA does not wait for all the responses before connecting OSwMI 1. Then the new calling party MS2 (MS2) joins the existing call, since OSwMI 2 is connected to the CSwMI/LMA. When all these SwMIs join the call including the newly joined OSwMI 2, ISI-Setup Acknowledge messages from different SwMIs should be received by the CSwMI/LMA. It means that different SwMIs are connected to the call, and the associated mobile users of these SwMIs can join the group call.

So after this step, RSVP-TE procedures are used to make the point to multipoint LSPs for the user data. The procedures are shown in the RSVP-TE box. When the point to multipoint LSPs are successfully reserved, the ISI-Connect messages are sent to the different SwMIs. Afterwards, group members get the D-Connect messages so that the connection between the calling user and the called users is made.

If the RSVP-TE procedure is unsuccessful then a similar unsuccessful procedure is used as the one described in Section 4.3.2.1.

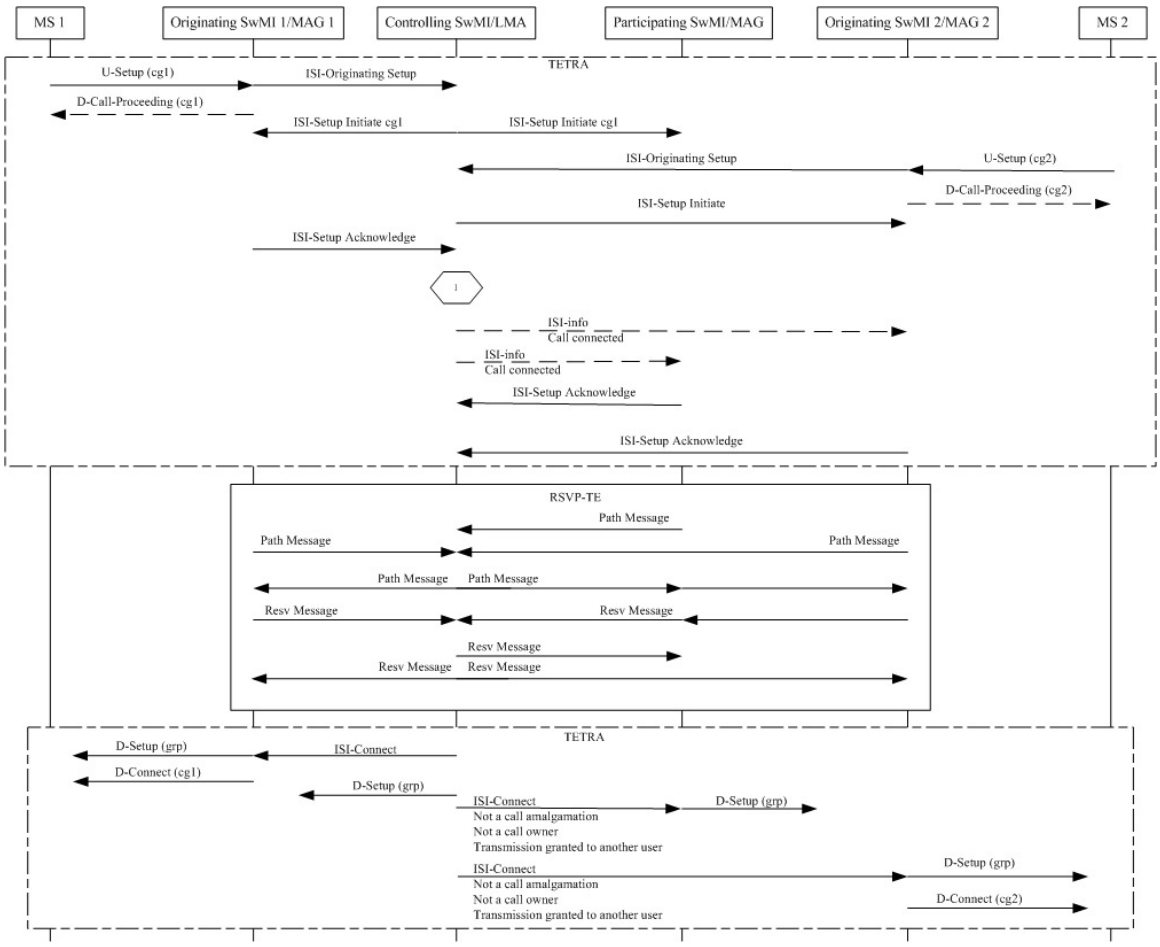

Figure 28: Multiple calling parties, a new calling party is on OSwMI2

4.3.2.4 Successful Group Call Establishment: only one calling party is accepted by the CSwMI

For this call setup scenario, one calling party that is connected to the PSwMI is willing to initiate a call, see Figure 29.This figure is made based on Figure E.14 in Annex E from [ETSI-EN-300392-3-3].

The MS1 initiates the call set-up by sending a U-Setup message to the Originating SwMI/MAG. The CSwMI/LMA gets ISI-Delay messages both from the Originating SwMI/LMA and the PSwMI since they are not yet ready. The CSwMI only accepts one calling party, which is MS1 in this case. Thus the CSwMI rejects the call set-up request from MS2. After the Originating SwMI/LMA sends an ISI-Setup-Acknowledge message to the CSwMI/LMA, the RSVP-TE starts to reserve the network resources. The RSVP-TE procedures are based on [RFC 3209] and [RFC 4875]. To do this, the OSwMI and PSwMI send a Path message towards the CSwMI. The CSwMI then starts to send the RSVP_Path* messages to the OSwMI and PSwMI.

If the RSVP-TE procedures are successful, then this will mean that the point-to-multipoint LSPs are made for transporting the user data using a bi-directional communication mode.

Then the CSwMI/LMA sends an ISI-Connect to the OSwMI so that the group members from the Originating SwMI/MAG are connected to the call. Similarly, the group members from the Participating SwMI/LMA also join the call.

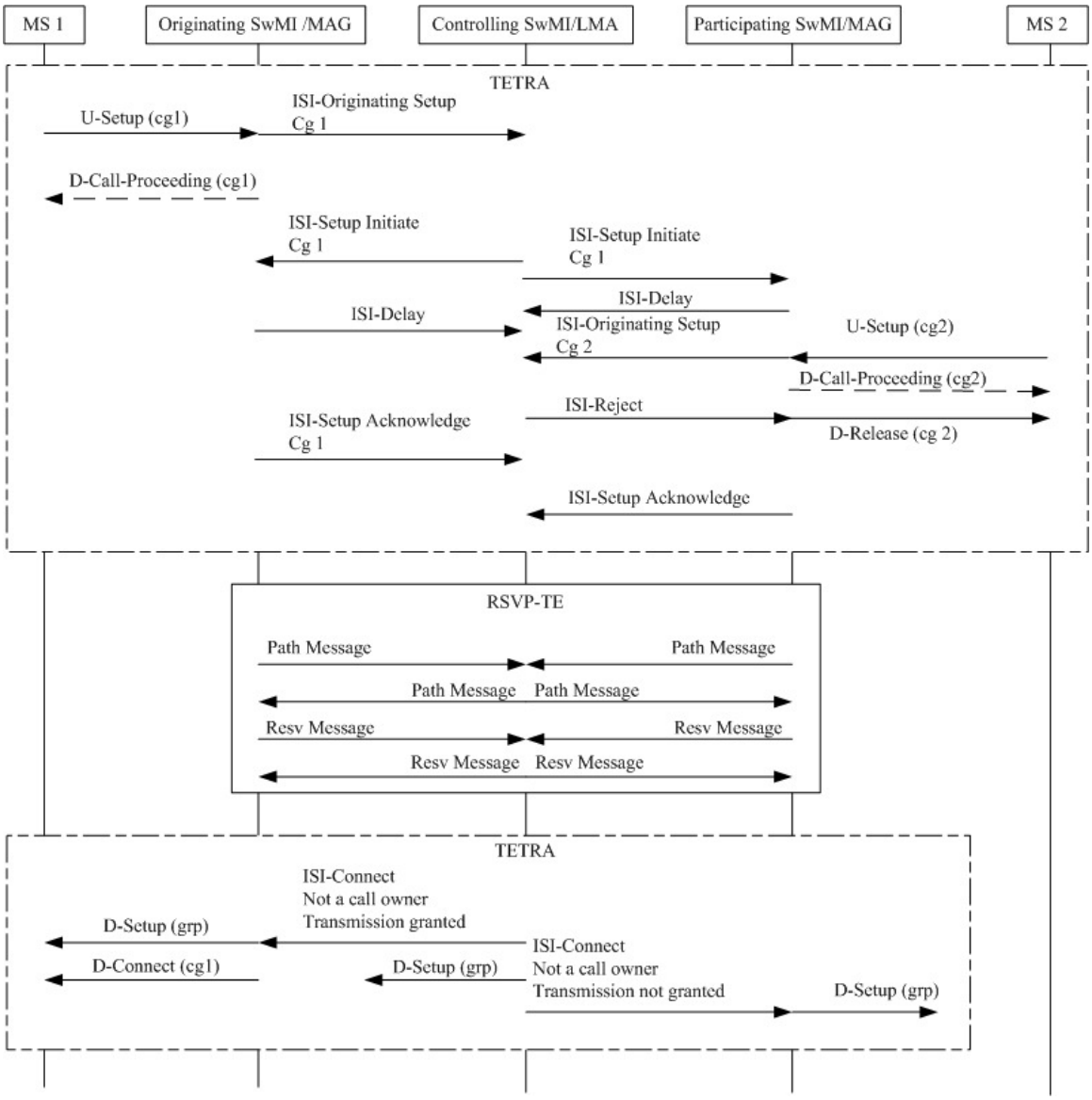

Figure 29: Successful group call set-up: CSwMI only supported one calling party

4.3.2.5 Late Entry

Late entry is a group call related service. Since late entry is a scenario that supports the functionality that a MS wants to join an existing call, it is considered that the late entry

procedure is a call setup scenario. This scenario is depicted in Figure 30. This figure is made based on Figure E.15 in Annex E from [ETSI-EN-300392-3-3].

Originally, the PSwMI1 is not involved in the call. In Figure 30, it is considered that a group of members are already attached to this Participating SwMI. After the call is connected, the CSwMI/LMA sends an ISI-Setup Initiate message to the PSwMI1 for the support of the Supplementary Service-Late Entry. Since the PSwMI1 cannot provide enough resources to connect it, an ISI-Delay is sent to the CSwMI/LMA. In general, one newly attached mobile user of the PSwMI1 can cause the CSwMI/LMA to send an ISI-Setup Initiate to the Participating SwMI. This could also be triggered by the expiration of a timer so that CSwMI has to re-evaluate the list of Participating SwMIs/MAGs. As long as the resources are ready for the call connection, the PSwMI1 sends ISI-Setup Acknowledge to the CSwMI/LMA.

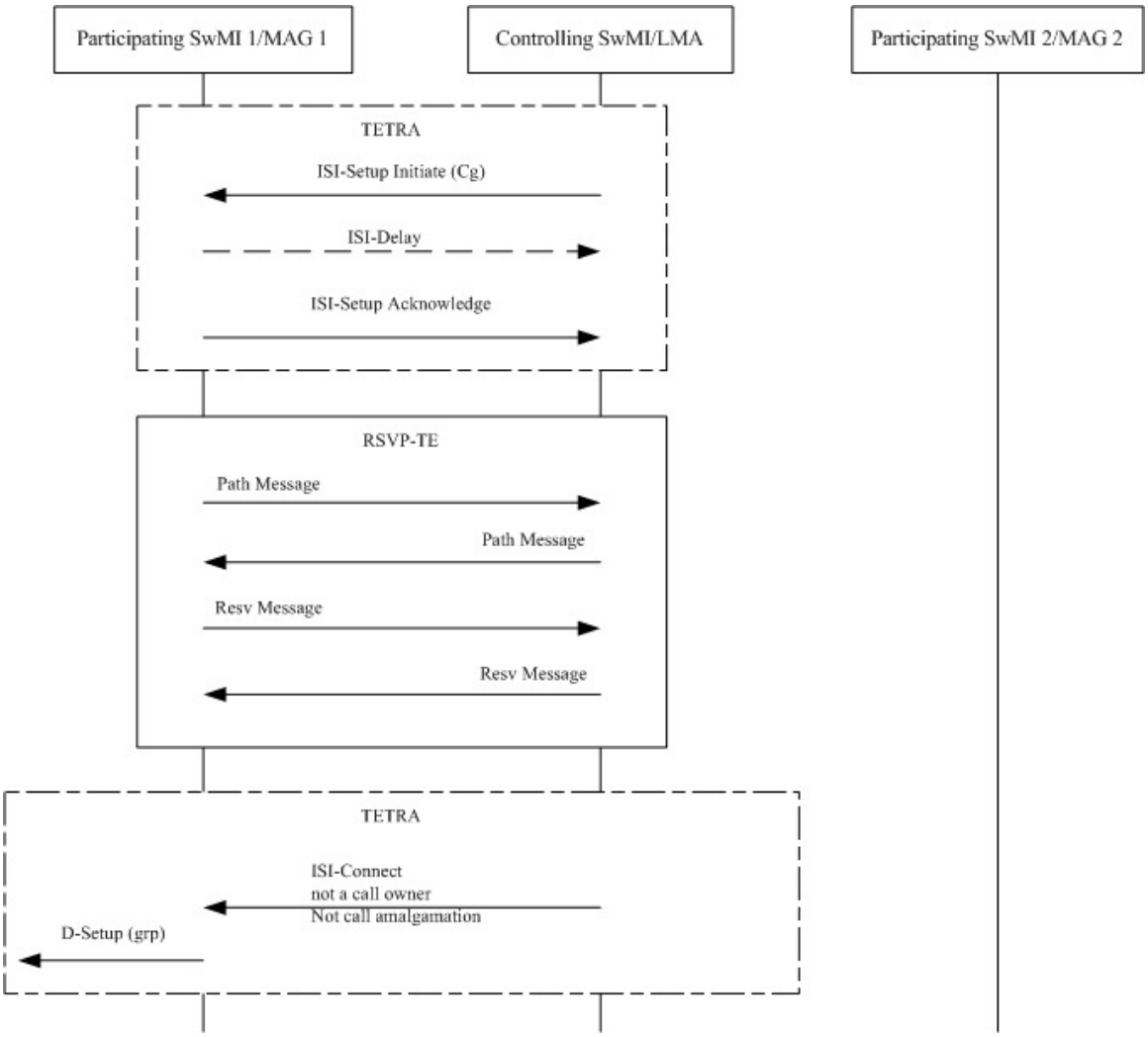

Figure 30: Late entry

After the first TETRA procedure box, the RSVP-TE procedures are used to set up the point-to-multipoint LSPs. The OSwMI/MAG first sends the RSVP_Path message to the CSwMI/LMA. The CSwMI then starts the RSVP-TE procedures in order to setup point-to-multipoint LSPs towards and from all the involved SwMIs

Subsequently, the CSwMI sends an ISI-Connect message to the OSwMI/MAG. Finally, the OSwMI sends the D-Connect or D-Setup messages to instruct this new MS to join the existing call.

4.3.2.6 A SwMI Joins a Connected Call

In this scenario, see Figure 31, the PSwMI/MAG and CSwMI/LMA are already in a group call whose calling party is at the OSwMI/MAG. A mobile station is the joining party that is not the initiator of the call. The MS sends the U-Setup in order to trigger that an ISI-Originating Setup is sent to the CSwMI/LMA. The CSwMI/LMA has the right to decide whether it wants to accept the joining request from the MS. In case the CSwMI/LMA does not accept the joining request, an ISI-REJECT is sent back to the OSwMI/MAG. In this figure, the OSwMI/MAG gets the ISI-Setup Initiate from the CSwMI/LMA. Moroever, the OSwMI/MAG is not ready to connect the MS to the existing call, so an ISI-Delay message is sent to the CSwMI/LMA. Once the OSwMI/MAG is ready to connect the MS to the existing call, it sends ISI-Setup-Acknowledge message to the CSwMI/LMA.

After this step, the RSVP-TE procedures are used to reserve the network resources for the user data are accomplished. These RSVP-TE procedures are exactly the same as in late entry.

If all the RSVP-TE procedures are successfully done, an ISI-Connect message is sent to the OSwMI to make the call amalgamation. Finally, D-Connect (cg) or D-Setup (grp) is sent to the MS such that it joins the existing call. For this scenario, if the joining mobile station or the OSwMI disconnect before it receives the D-Connect, only this part of the whole connection is released, rather than the whole connection. In short, upon receiving the ISI-Originating Setup for an existing group call, the CSwMI/LMA may allow the party to join in the existing call. This can be done by initiating a call with joining SwMI only.

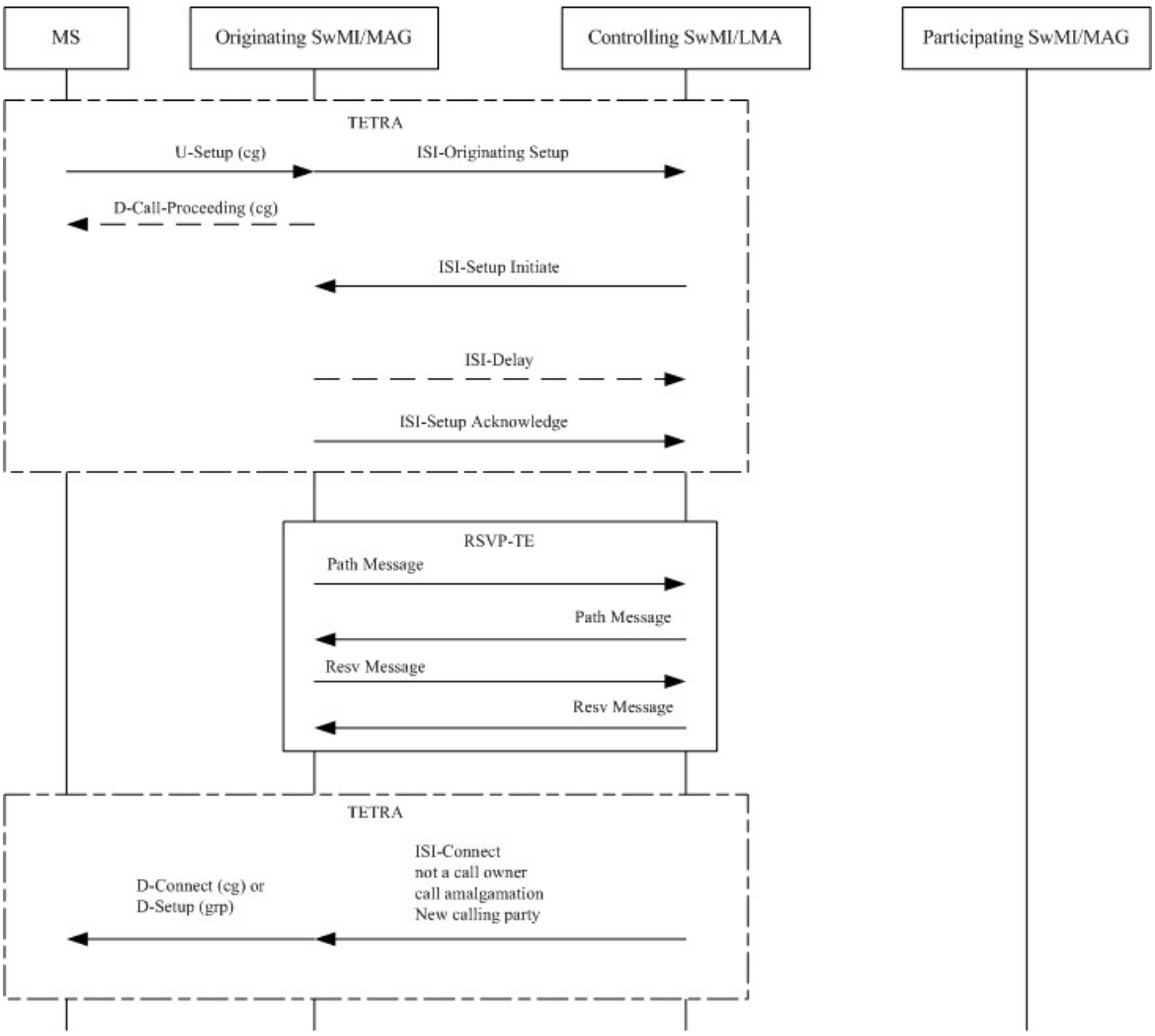

Figure 31: A Party joins with a connected call

4.3.2.7 An Emergency Priority Call to a Group that is already active in a call

This scenario is relevant to the pre-emption call. Consider we have one existing group call (call 1). A mobile user wants to make an emergency call to a group. See Figure 32 for a depiction of this call set-up scenario.

The PSwMIs/MAGs and CSwMI/LMA are already active in a group call, Call 1, which is a non-emergency call. One party at the OSwMI/MAG wants to make an emergency call to the group that is already in the group Call 1. So this party sends U-Setup to the OSwMI (Call 2). This action triggers CSwMI/LMA to send ISI-Setup Initiate for the new call (an emergency priority call) to the OSwMI/MAG and PSwMI/MAG. After sending the ISI-Setup Initiate, the CSwMI/LMA tries to release the call 1. After the ISI-Release message arrives at OSwMI (call 2) and PSwMI/MAG, RSVP-TE starts to tear down the

communication paths for the Call 1, using RSVP_PathTear* messages, so that the network resources can be released.

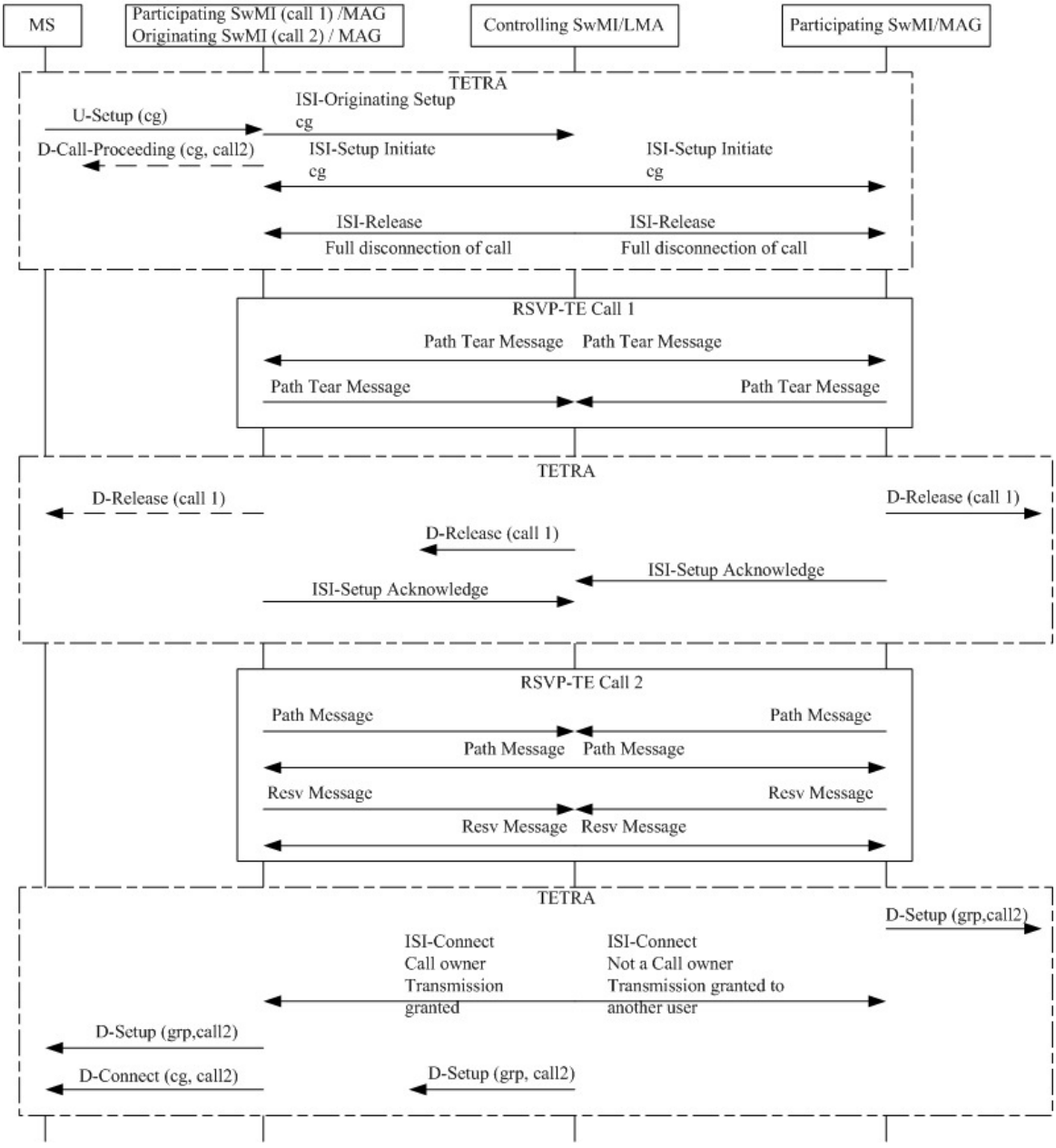

Figure 32: An emergency priority call to a group that is already active in a call

Then the second TETRA procedure box shows the D-Release messages are sent to the group members of the Call 1. Afterwards, OSwMI (call 2) and PSwMI/MAG send ISI-Setup Acknowledge to the CSwMI/LMA. So the RSVP-TE procedures are performed to make set-up the point-to-multipoint LSPs that can be used in a bidirectional communication mode for the group call 2. When the point-to-multipoint LSPs are set up

successfully, then the last TETRA procedure box has to be used to inform all the group members that they are connected to the group Call 2.

4.3.2.8 Partial Successful Group Call Establishment

This call setup scenario is used when one mobile user sets up the call, and one participating SwMI/MAG rejects this call. So only part of the group members are connected to the call. Figure 33 depicts this scenario.

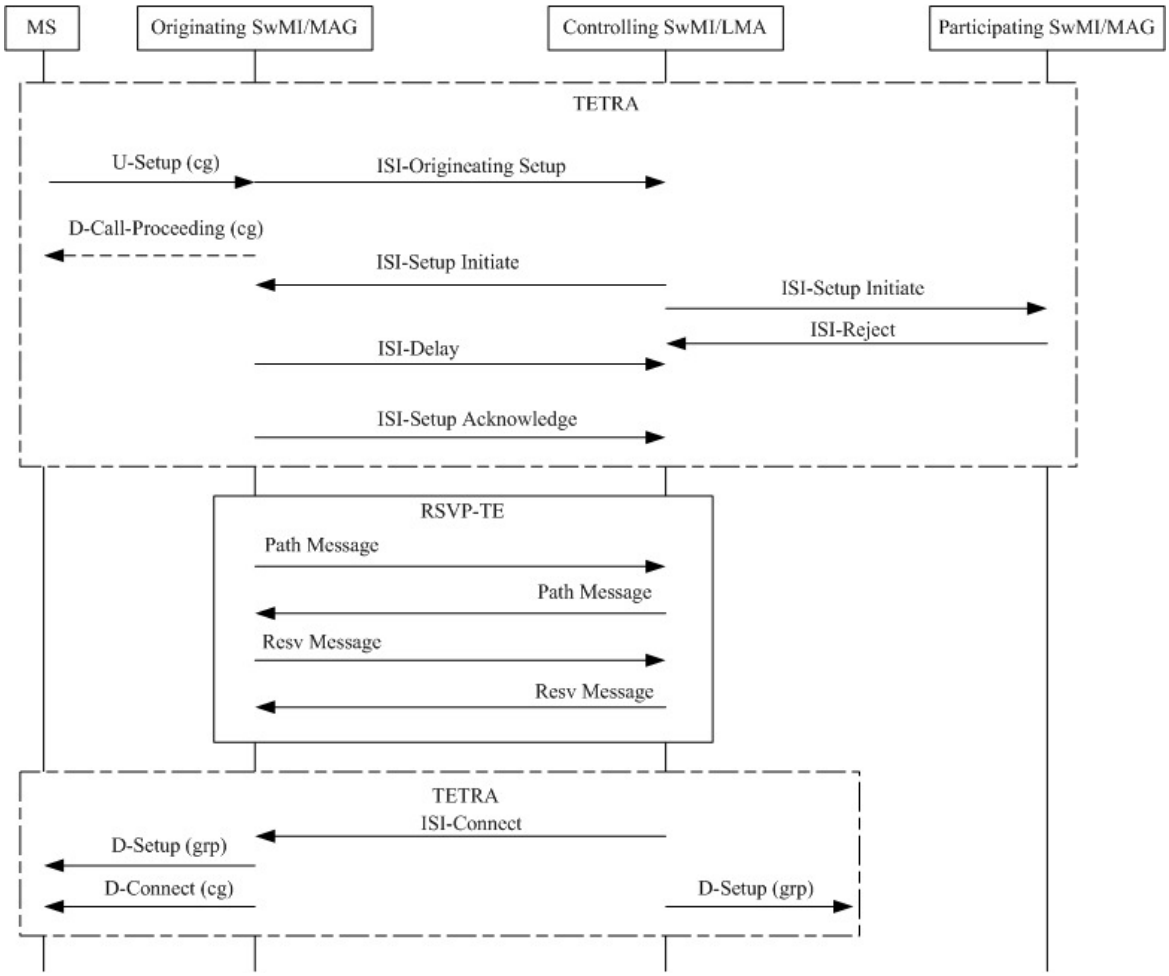

Figure 33: Partial successful group call setup

In the first TETRA box, an MS sends U-Setup message to OSwMI/MAG. Then the OSwMI/MAG sends the ISI-Originating Setup message to the CSwMI to trigger it. Then the CSwMI/LMA sends ISI-Setup Initiate messages to the OSwMI/MAG and PSwMI/MAG respectively. After this step, the OSwMI/MAG and PSwMI/MAG give feedback for the ISI-Setup Initiate. The PSwMI/MAG rejects the setup request while OSwMI/MAG is not ready to connect the call. After a while, OSwMI/MAG is ready for the connection, so it sends an ISI-Setup Acknowledge message to the CSwMI/LMA.

Now the RSVP-TE procedures are started in order to set-up the point-to-multipoint LSPs between the OSwMI/MAG and CSwMI/LMA, see previous sections.

Since CSwMI/LMA receives feedback from both OSwMI/MAG and PSwMI/MAG, it knows that it can only connect the OSwMI/MAG and not the PSwMI/MAG. Thus CSwMI/LMA sends ISI-Connect to the OSwMI/MAG and D-Setup to the group members who are attached to the CSwMI/LMA. Then the OSwMI/MAG sends D-Setup messages to the mobile station. Since there are other group members that are attached to the OSwMI/MAG, the OSwMI/MAG connects these group members by sending D-Connect messages.

4.3.2.9 Unsuccessful Group Call Establishment

In the section 4.3.2.1, we show an example of unsuccessful group call setup that is caused by the fact that the RSVP_Path* message cannot be satisfied. In addition to this type of unsuccessful group call establishment, other unsuccessful group call establishment cases can occur. Basically, there are three cases: 1. Unsuccessful group call establishment due to the rejection by an OSwMI/MAG. 2. The CSwMI/LMA cannot accept some parameters. 3. Unsuccessful group call establishment due to the rejection by a CSwMI/LMA. All these three scenarios only need TETRA procedures, so the figures in this section are the original figures from [ETSI-EN-300392-3-3].

The first unsuccessful group call setup scenario is shown in the Figure 34.

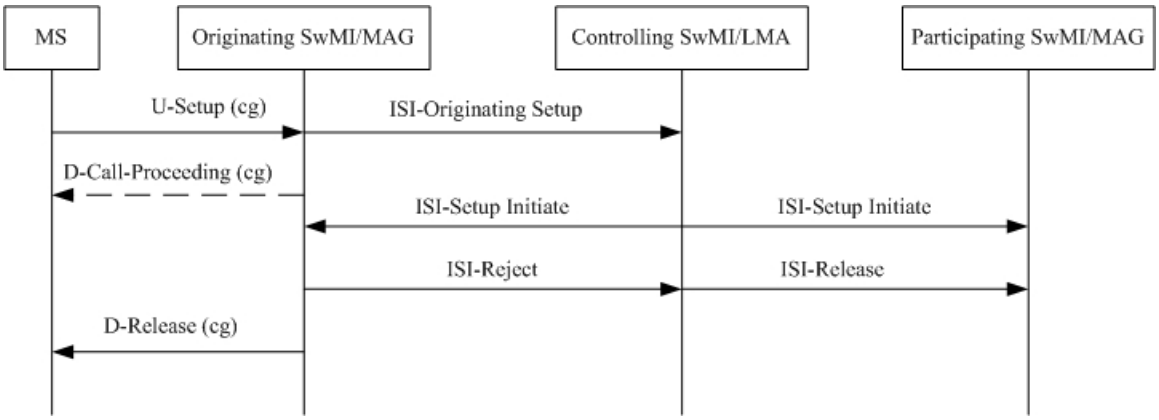

Figure 34: Unsuccessful group call setup, rejected by an OSwMI

This figure is exactly the same as in figure E.20 unsuccessful group call establishment, rejected by a SwMI from [ETSI EN 300 392-3-3]. In this scenario, a mobile station wants to set up the group call. However OSwMI rejects the ISI-Setup Initiate that is sent by the CSwMI. Since there are no other calling parties, the group call can not be made. The CSwMI releases the other PSwMIs from the group call by sending ISI-Release.

The second unsuccessful group call setup scenario is that the CSwMI cannot accept some parameters for instance resource allocation that should be included in the ISI-Setup Acknowledge. This scenario is shown in Figure 35.

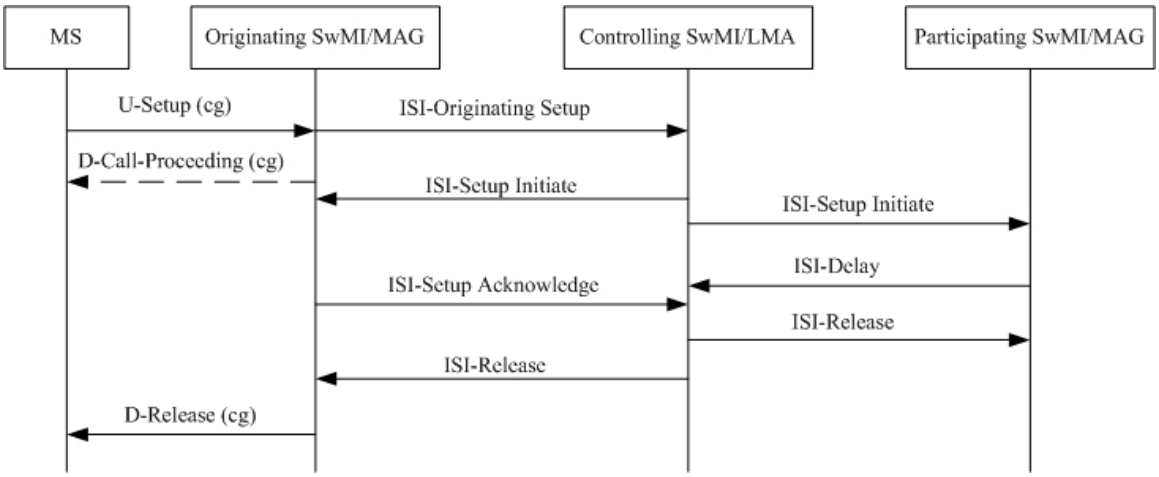

Figure 35: Unsuccessful group call setup, the CSwMI cannot accept some parameters

If the OSwMI/MAG requests a different communication type rather than point-to-multipoint or it does not support a resource allocation mode in its ISI-Setup Acknowledge, the CSwMI cannot accept this ISI-Setup Acknowledge. So the CSwMI/LMA releases all the SwMIs.

The third scenario happens when the ISI-Originating Setup is declined by the CSwMI/LMA, see Figure 36.

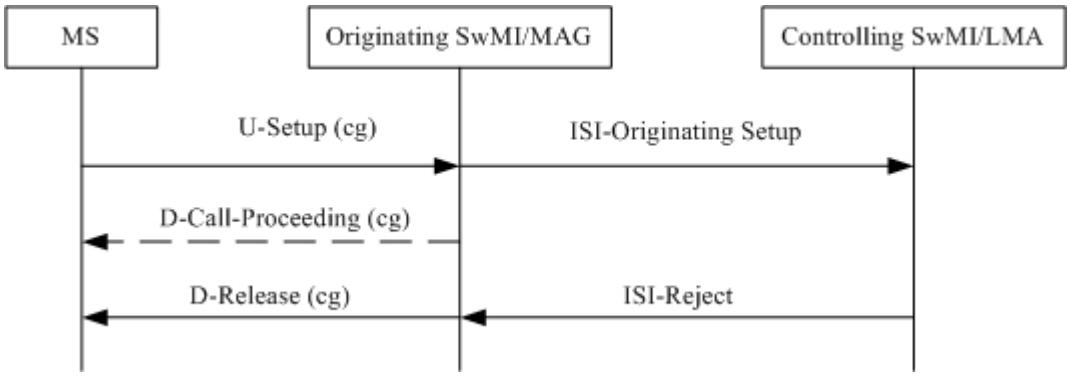

Figure 36: Unsuccessful group call setup, rejected by the CSwMI

This scenario is quite straight forward. Once the CSwMI/LMA receives an ISI-Originating Setup message that cannot be satisfied, then the CSwMI rejects this setup request.

4.3.3 Call Maintenance: Push to Talk (PTT)

After call establishment, a user needs to start a call maintenance procedure, e.g., push to talk service, before being able to send user data (speech or video) towards all the other group members. Push to talk (PTT) is a way of transmitting user data, where a user informs all the other group members that he/she will start sending user data. This will mean that during this period all the other group members will not be able to send any data on the communication medium allocated for this group.
We distinguish two ways of implementing the PTT procedure: the standard TETRA way (i.e., normal way) and a new way that is specified in [ODINI_patent]. We denote this PTT as the ODINI way. The PTT *normal way* is based on the TETRA call maintenance procedure depicted in Figure E.24 from [ETSI-EN-300392-3-3] and the PTT *ODINI way* is based on [ODINI_patent].

ODINI is considered to be a middle-layer protocol that can support various application scenarios with the goal to accomplish mission-critical group communications. The basic idea of ODINI is that it is built on top of IP to support all kinds of network scenarios that are described in section 2.2. The main functionalities of ODINI are group/individual voice calls, data transmission, roaming, networking based on IP multicast, interworking with a gateway. In our architecture, we only use the ODINI Push to talk operation that will be part of the *Interworking* function used in the Gateway, see Section 4.2.1.1.

As mentioned earlier, in [ETSI-EN-300392-3-3], there are two resource allocation policies for a PSwMI to allocate resources: 1) permanently allocated resources policy; 2) temporary allocated resources policy.
For the permanently allocated resources policy, all resources reserved during call set-up should be available for the call maintenance. So during the call maintenance, we do not need to reserve the resources. For the temporary allocated resources policy, during the call maintenance the CSwMI/LMA has to use RSVP-TE procedures to set-up the LSPs and assign the requested resources.

Considering that we have two ways to perform PTT and two resource allocation policies, so we have four cases for achieving PTT:

1. Normal way for PTT when using the permanently allocated resources policy;
2. ODINI way for PTT when using the permanently allocated resources policy;
3. Normal way for PTT when using the temporary allocated resources policy;
4. ODINI way for PTT when using the temporary allocated resources policy.

We will explain these four cases by using message sequence charts. The notations that are used in all the figures concerning all the PTT figures are as follows:

- ou stands for other user;
- qd stands for queued;
- gr stands for granted;
- ngr means not granted;
- pp stands for preemptive priority.

4.3.3.1 PTT Normal way when using permanently allocated resources policy

In TETRA, a demand to talk is considered to be the normal way for achieving PTT. The *normal way* of doing Push to Talk is part of call maintenance; see also Figure E.24 in [ETSI-EN-300392-3-3]. When the permanently allocated resources policy is adopted, all resources such as air interface, mobile and infrastructure resources that are reserved at the call set-up phase should be available for call maintenance. Since the normal way of doing Push to Talk is part of the call maintenance, so we do not need to use the RSVP-TE procedures to reserve the resources.

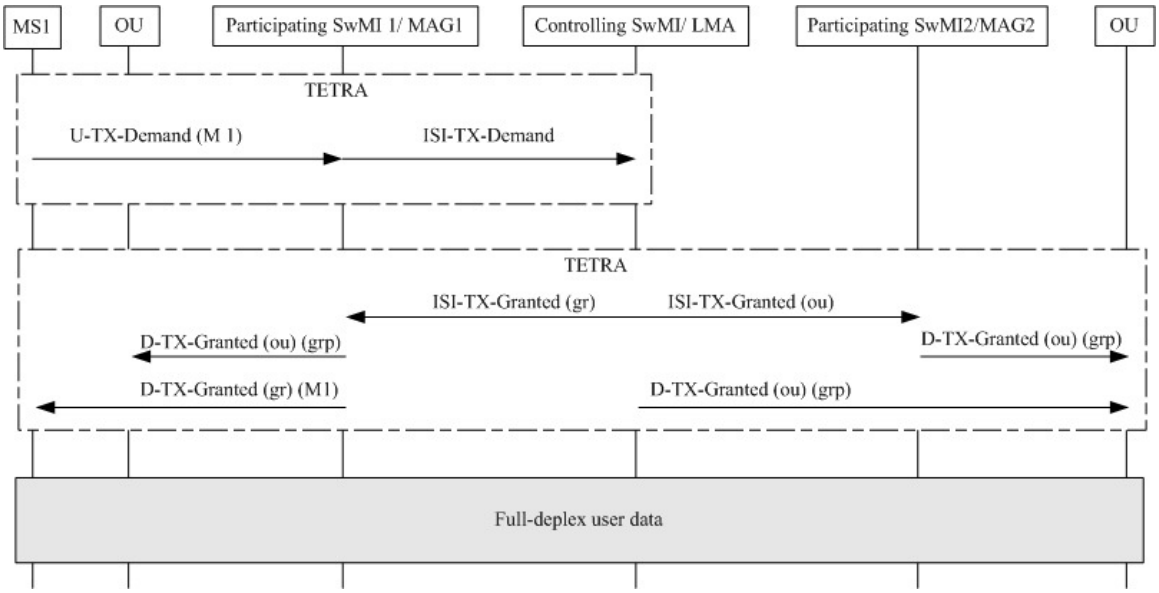

Figure 37: PTT normal way when using permanently allocated resources policy

In fact, Figure 37 shows the same signaling procedures as given in Figure E.2 in [ETSI-EN-300392-3-3]. When the PSwMI receives a U-TX-Demand message from MS1, it sends an ISI-TX-Demand message to the CSwMI/LMA. Then the CSwMI/LMA sends the ISI-TX-Granted and ISI-TX-Granted (ou) messages to the PSwMI 1 and PSwMI 2, respectively. These two PSwMIs/MAGs notify MS1 and other group members by sending D-TX-Granted messages. When all the group members are granted the permission to transmit, the MS1 can start to talk.

4.3.3.2 PTT ODINI way when using permanently allocated resources policy

Figure 38 shows the ODINI way for PTT when permanently allocated resources policy is adopted. This procedure is based on [ODINI_patent] and [ETSI-EN-300392-3-3].

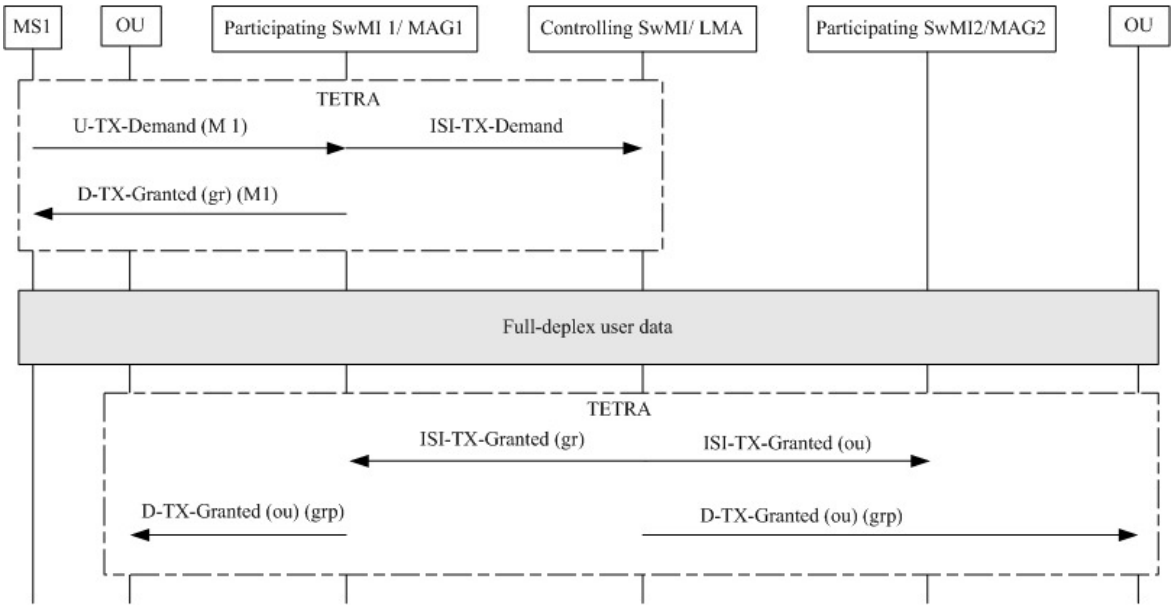

Figure 38: PTT ODINI way when using permanently allocated resources policy

The main difference between the PTT *normal way* and the PTT *ODINI way* is that in *ODINI way* the Participating SwMI, directly informs MS1 that it can start transmission (by sending a (D-TX-Granted (gr)M1) after receiving the U-TX-Demand message from MS1. Once the mobile station receives the transmission granted message D-TX-Granted from the Participating SwMI, it can start the user data transmission. Since the resources are already reserved during the call setup, the RSVP-TE will not be used.
As can be seen in Figure 38, MS1 first sends U-TX-Demand message to the PSwMI1 (PSwMI 1)/MAG.

In parallel, PSwMI 1/MAG sends the ISI-TX-Demand to the CSwMI/LMA and grants the transmission permission by sending D-TX-Granted to MS1. At this point, MS1 can start to talk. During the transmission, the CSwMI/LMA informs all the involved PSwMI/MAG that MS1 is allowed to talk by sending ISI-TX-Granted messages. Afterwards, the PSwMIs transmit D-TX-Granted to other users. After this point, all the group members can receive the user data sent by MS1.

4.3.3.3 PTT Normal way when using temporary allocated resources policy

The PTT normal way that uses the temporary allocated resources policy is similar to the one described in Section 4.3.3.1.

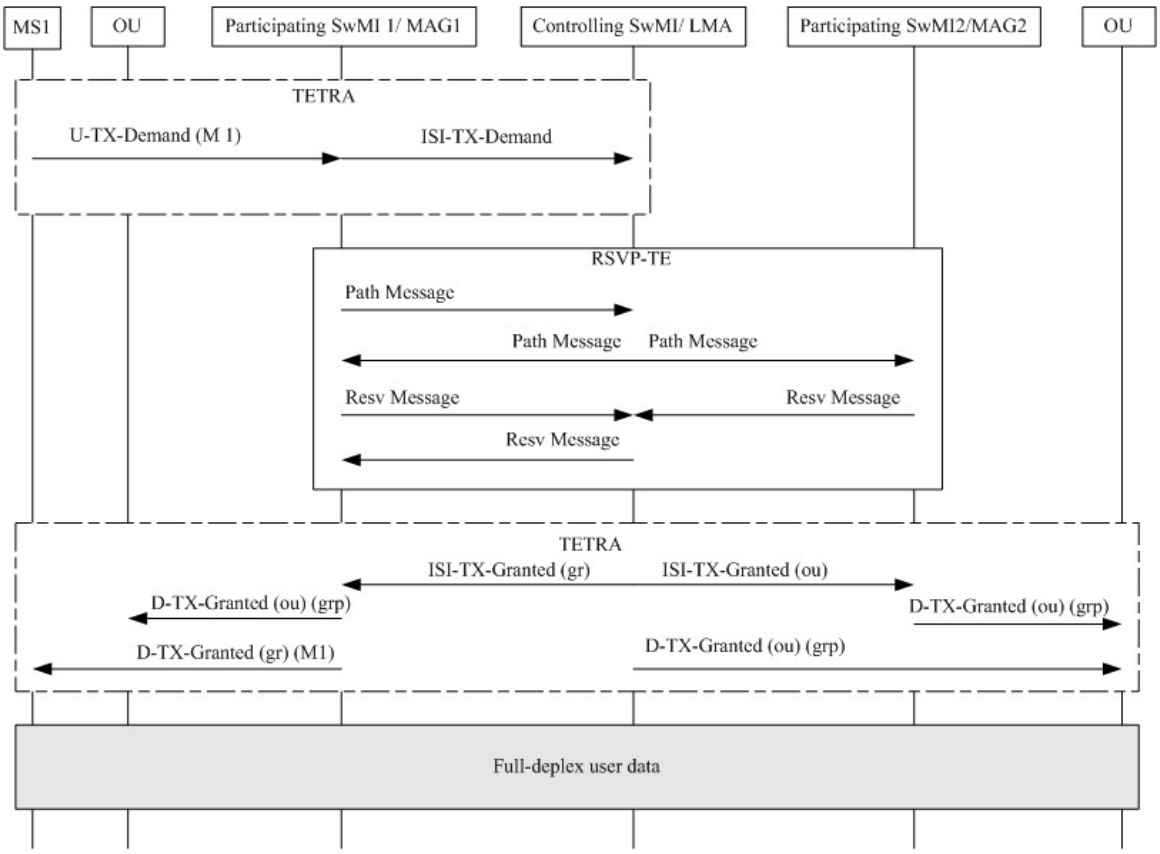

Figure 39: PTT Normal way when using temporary allocated resources policy

The only difference between this PTT *normal way* case and the PTT normal way case when using the permanent allocated resources policy, is that in this case the LSPs for the user data and their required resources need to be reserved before the transmission of user data starts. The first TETRA signaling box, see Figure 39, shows the situation that MS1 initiates the push to talk by sending a U-TX-Demand message to the PSwMI 1. Then the PSwMI 1/MAG sends an ISI-TX-Demand message to the CSwMI/LMA, which triggers the ISI signaling messages to be sent in the core network afterwards.

Since MS1 is the transmitter, in order to set-up a point-to-multipoint LSP for the user data, the hosting PSwMI/MAG (PSwMI 1) starts the RSVP-TE procedures by sending RSVP-Path message to the CSwMI/LMA. Then the CSwMI/LMA knows it needs to make a point-to-multipoint LSP between the CSwMI/LMA and the other SwMIs/MAGs, see e.g., Section 4.3.2.1. If the RSVP-TE procedure is successful then the LSPs required between the different SwMIs are set-up and the required resources are allocated. CSwMI

The second TETRA procedure box shows the ISI signaling messages to be sent in the core network. The CSwMI/LMA sends the ISI-TX-Granted and ISI-TX-Granted (ou) to PSwMI 1 and PSwMI 2, respectively. These two PSwMIs/MAGs notify MS1 and other group members about the situation that MS1 will start transmitting user data, by sending D-TX-Granted. The CSwMI/LMA also sends the D-TX-Granted to the group members that are attached to the CSwMI.

4.3.3.4 PTT ODINI way when using temporary allocated resources policy

The PTT *ODINI way* when using the temporary allocated resources policy is similar to the one described in Section 4.3.3.2.

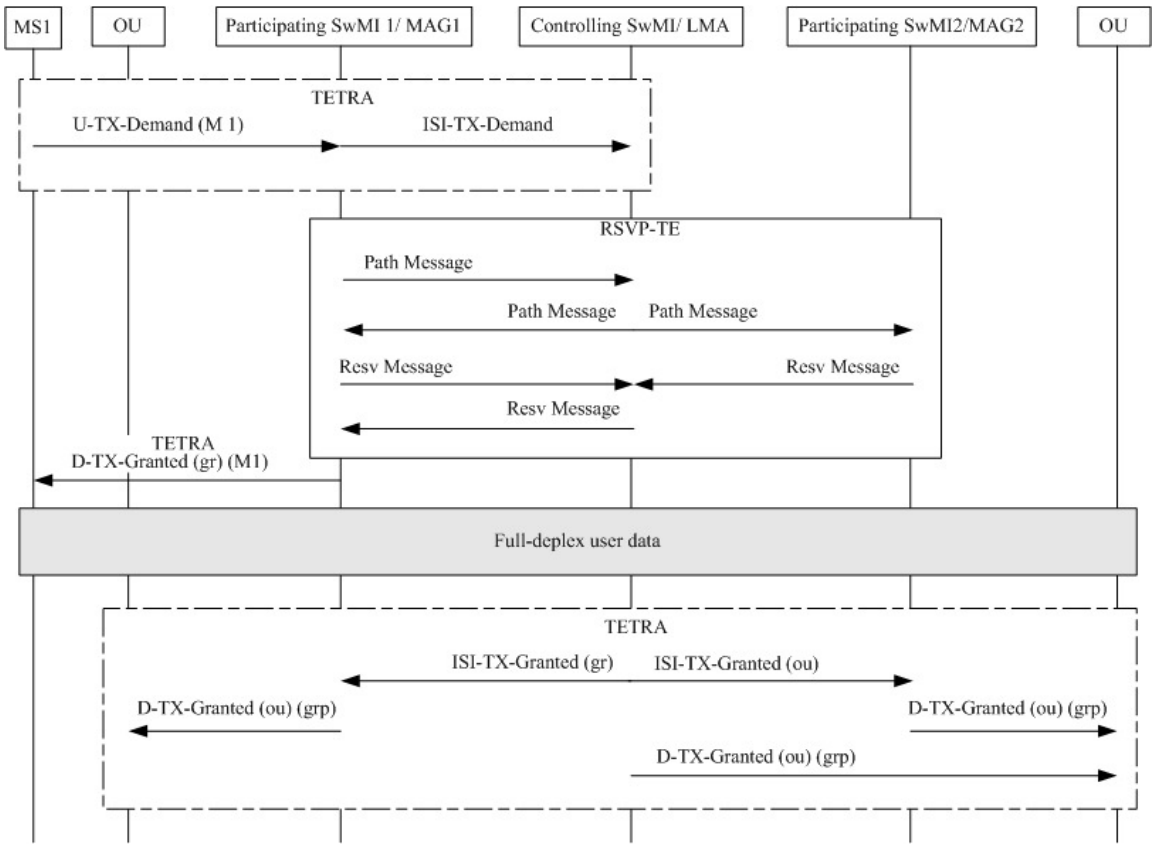

Figure 40: PTT ODINI way when using temporary allocated resources policy

Compared with the PTT *ODINI way* described in Section 4.3.3.2, in this PTT *ODINI way* case, RSVP-TE procedures are required to set-up the required LSPs and to reserve the required resources before the transmission starts.

After the first TETRA signaling box is completed, see Figure 40, RSVP-TE procedure is used, which is similar to the one described in Section 4.3.3.3.

The second TETRA signaling box shown in Figure 40, it is similar to the second TETRA signaling box given in Figure 38.

4.3.3.5 Unsuccessful Push to Talk Scenarios

In this section, only the unsuccessful PTT normal way and PTT ODINI way push to talk scenarios when using the temporary allocated resources policy are discussed.

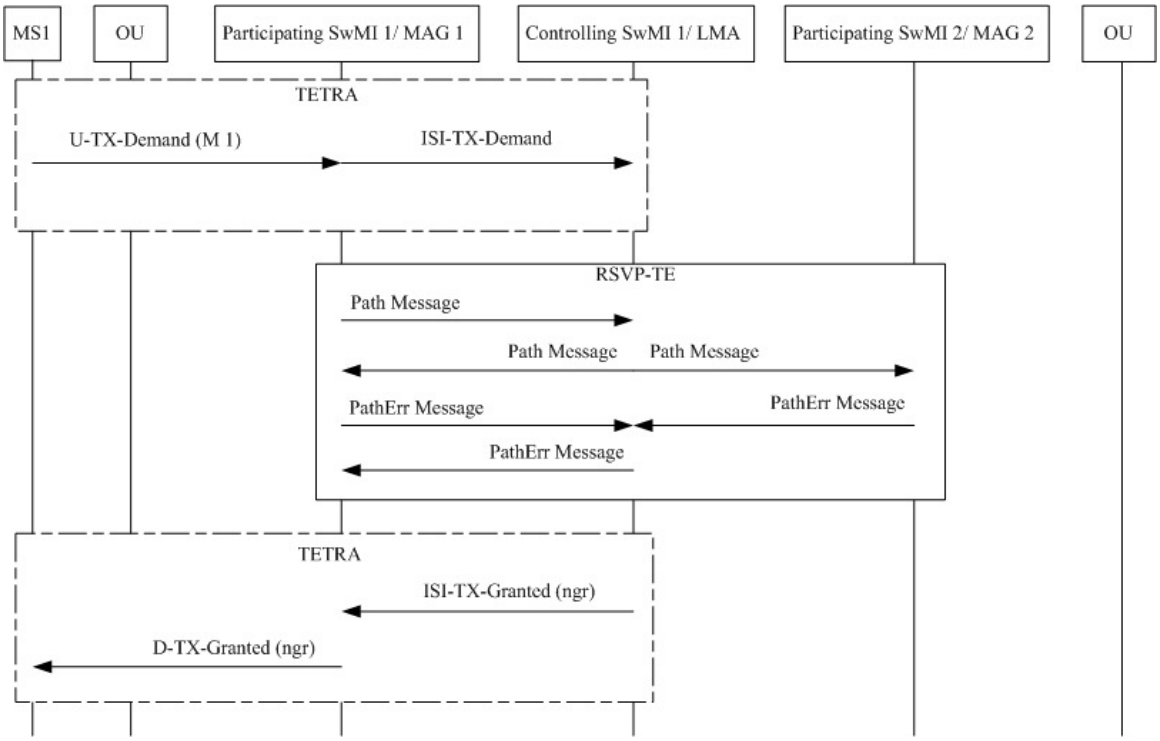

Figure 41: Unsuccessful PTT normal way when using temporary allocated resources policy

In the unsuccessful PTT normal way scenario when using temporary allocated resources policy, see Figure 41, once the CSwMI/LMA receives an ISI-TX-Demand from the PSwMI1/MAG 2, the RSVP-TE starts to set-up point-to-multipoint LSPs. However, if the RSVP-TE procedure is unsuccessful then CSwMItwo RSVP_PathErr* messages are sent towards the CSwMI 1/LMA. Afterwards, PSwMI1/MAG 2 is aware that the resources are not reserved successfully since it receives a PathErr message from the CSwMI 1/LMA. Then the second TETRA procedure box starts. In this part, since the CSwMI 1/LMA knows the result of resource reservation, it informs the PSwMI1/MAG 1 that transmission is not granted. Finally the PSwMI1/MAG 1 informs the MS1 that it cannot start transmission by sending D-TX-Granted (ngr).

The second unsuccessful scenario that is described in this section is the *u*nsuccessful PTT ODINI way when using the temporary allocated resources policy, see Figure 42. In fact, the only difference between this unsuccessful scenario and the one depicted in Figure 25 is related to the moment that the PSwMI1/MAG1 sends a D-TX-Granted message to MS1.

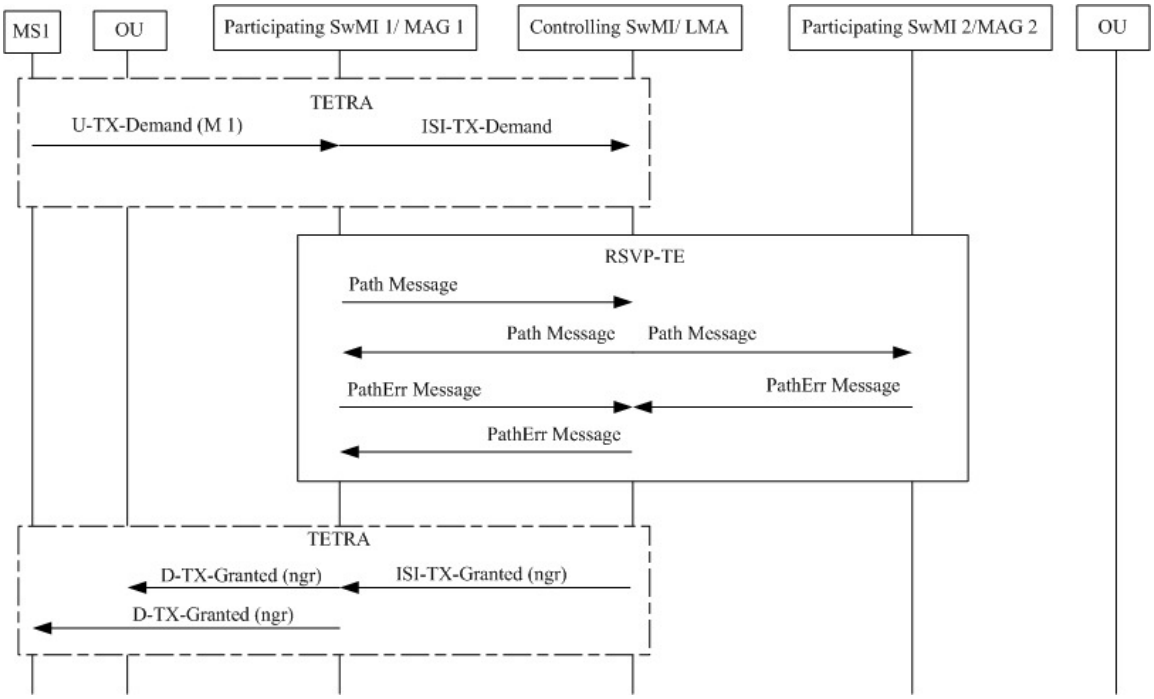

Figure 42: *U*nsuccessful PTT ODINI way when using *temporary allocated resources policy*

4.3.4 Other Call Maintenance Procedures

In addition to the push-to-talk procedures described in the previous subsection other call maintenance procedures can also be identified, see Figure E.24 in [ETSI-EN-300392-3-3]. This section describes such call maintenance procedures, considering that the temporary allocated resource policy is supported.

The following call maintenance procedures that use the temporary allocated resource policy will be described in this section see also Figure E.24 in [ETSI-EN-300392-3-3]:

1. Talking party relinquishes the right to transmit. No queued demands.
2. A party, M 2, demands to talk and is queued since the MS1 is talking.
3. MS1 demands to talk at preemptive priority while MS2 has talk permission.
4. MS1 ceases.
5. MS4, present at the CSwMI requests to talk at preemptive priority.
6. MS4 ceases.

Figure 43 depicts the message sequence chart associated with the first call maintenance procedure given above.

.

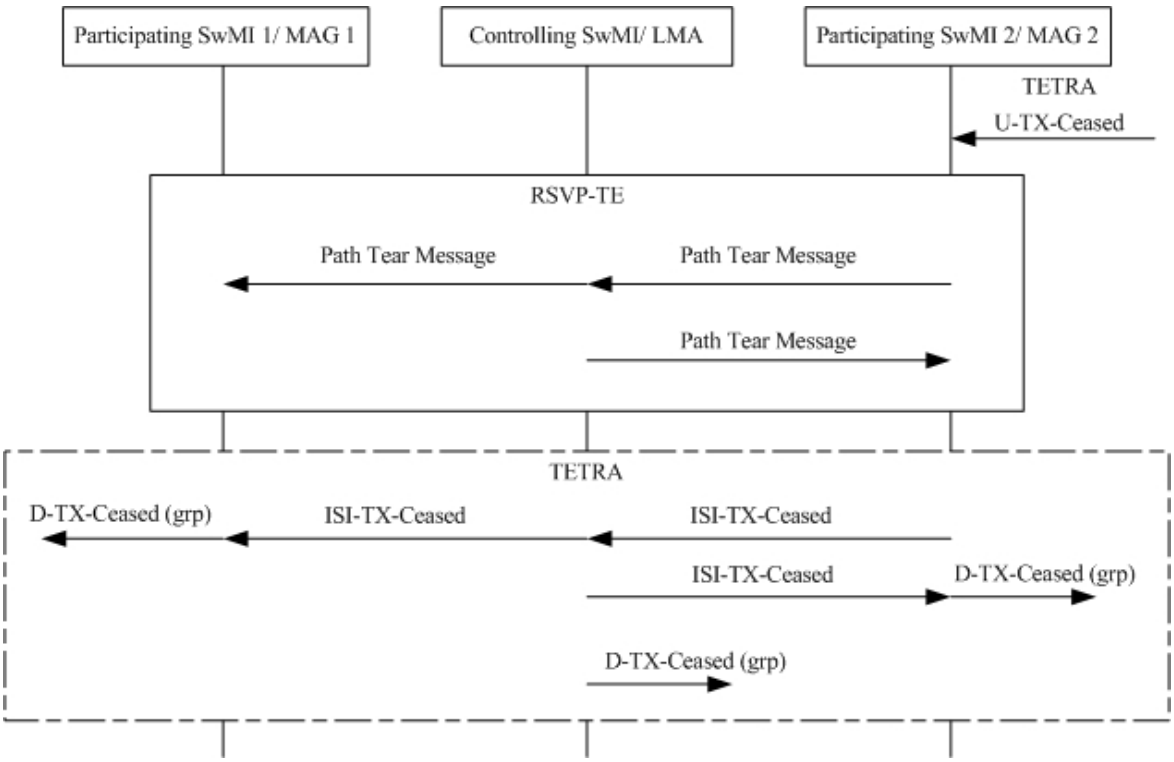

Figure 43: Talking party relinquishes the right to transmit. No queued demands

One talking party that is attached to the PSwMI2/MAG 2 is willing to stop transmitting information. This will mean that the reserved resources associated with this party have to be released. This can be realized by using the tear down procedures of RSVP-TE to release the resources associated with this party. Upon receiving U-TX-Ceased from the talking party, the Participating SwMI (PSwMI) 2/MAG 2 sends the RSVP_Path Tear message to the CSwMI/LMA. The CSwMI/LMA will release the resources that are reserved along the multicast path by sending RSVP_PathTear* message to the PSwMI1/MAG 1 and PSwMI2/MAG 2. Subsequently, the PSwMI2/MAG 2 starts the TETRA procedures by sending an ISI-TX-Ceased message to the CSwMI/LMA. Then the CSwMI/LMA notifies the group members about the modified situation via the two PSwMIs. After receiving the ISI-TX-Ceased, the two PSwMIs cease the attached group members. Finally the CSwMI/LMA ceases the group members that are attached to the CSwMI/LMA.

Figure 44 shows a call maintenance procedure, where a MS, e.g., MS2, is willing to talk, but it is blocked/queued due to the fact that another MS, e.g., MS1, is at that moment talking. The procedure shown in Figure 44 is identical to the same procedure shown in Figure E.24 that is given in [ETSI-EN-300392-3-3].

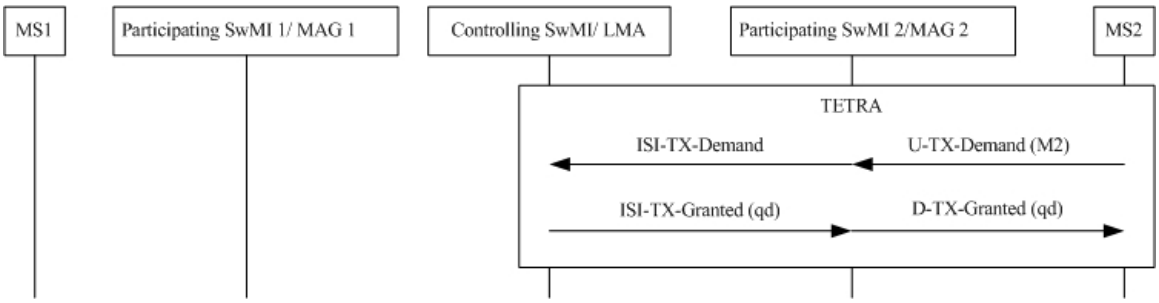

Figure 44: A party, MS2, demands to talk and is queued since the MS1 is talking

Figure 45 shows the situation that a MS, i.e., MS1 demands to talk at preemptive priority while another MS, i.e., MS2 has already permission to talk.

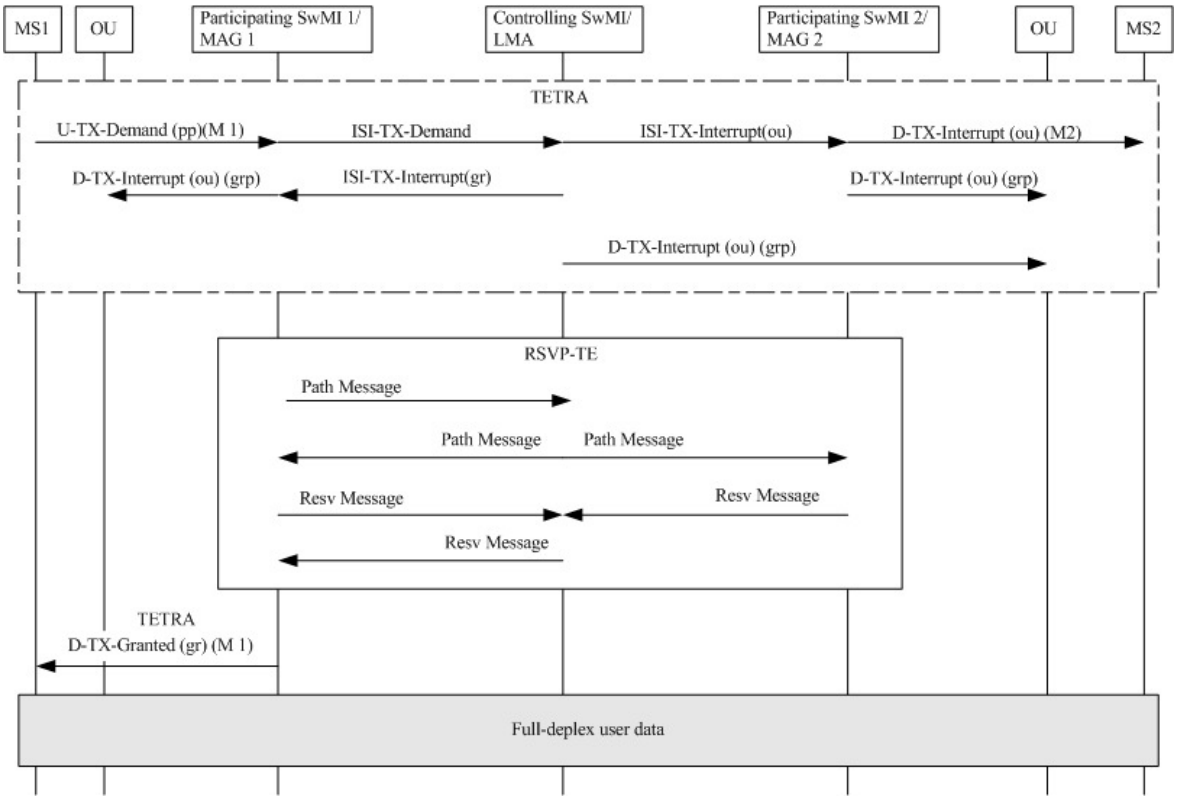

Figure 45: MS1 demands to talk at preemptive priority while MS2 has talk permission

In this procedure, MS1 sends the U-TX-Demand message with preemptive priority to the PSwMI1/MAG 1. Then ISI-TX-Demand message is sent to the CSwMI/LMA. Consequently the CSwMI/LMA realizes that it needs to interrupt the transmission between MS2 MS2and other users. As we can see in the TETRA procedure box, all the group members receive the D-TX-Interrupt message either from the PSwMIs or the CSwMI. Subsequently, the RSVP-TE procedures start to make point-to-multipoint LSPs, since MS1 will become the transmitting MS. Upon receiving the RSVP_Resv message from the CSwMI1/LMA, the PSwMI1/MAG 1 grands the transmission permission to the MS1.

Figure 46 shows the situation that MS1 ceases transmission.

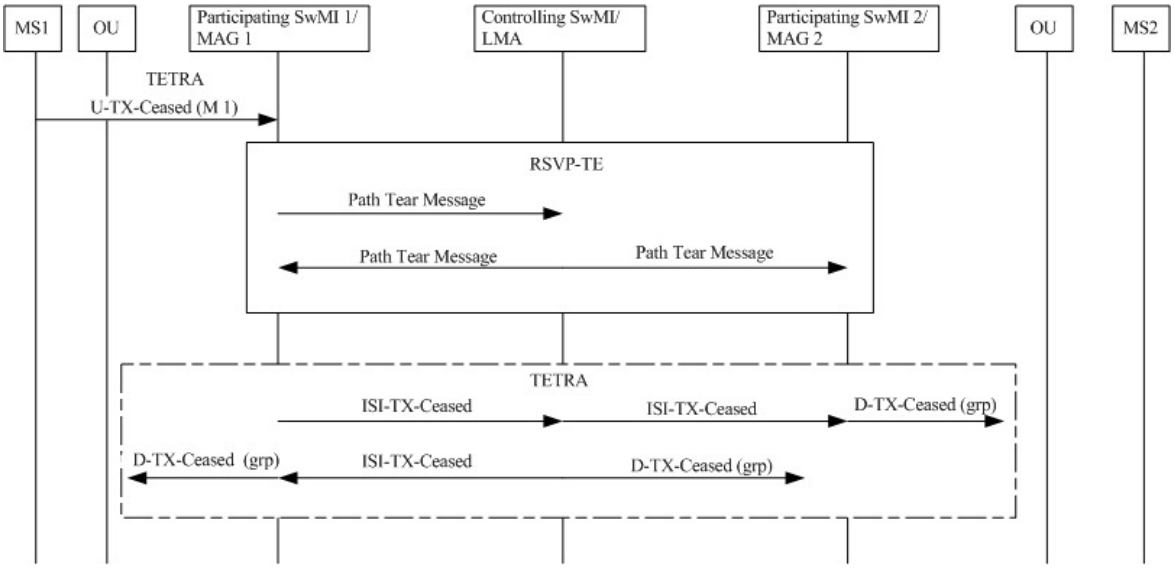

Figure 46: MS1 ceases

In this procedure, the MS1 ceases transmission by sending a U-TX-Ceased message to the PSwMI1/MAG 1, which triggers the RSVP-TE procedures to release the resources. To release the resources, the PSwMI1/MAG 1 first sends a RSVP Path Tear message to the CSwMI/LMA. The CSwMI/LMA releases the point-to-multipoint LSPs, which start from the CSwMI towards the two PSwMIs. When the resources have been released, the last TETRA procedure box starts to cease all the group members. The PSwMI1/MAG 1 first sends the ISI-TX-Ceased message so that CSwMI is notified that it needs to cease all the group members that that are attached to the different PSwMI and to itself. Thus the CSwMI sends ISI-TX-Ceased to the PSwMI 1 and PSwMI 2. These two PSwMIs cease their group members by sending D-TX-Ceased to all group members. The group members belonging to the CSwMI are ceased upon receiving the D- TX-Ceased message from the CSwMI.

Figure 47 shows the situation that a MS, i.e., MS4 present at the CSwMI requests to talk at preemptive priority. MS4 sends a U-TX-Demand message with pre-emptive priority to the CSwMI/LMA such that CSwMI/LMA is triggered to interrupt the transmission of the other users and MS3. So the CSwMI/LMA sends ISI-TX-Interrupt messages to the PSwMI 1/MAG 1 and PSwMI 2/MAG 2. Afterwards, these two PSwMIs can interrupt the communication of other users controlled by these PSwMIs by delivering the D-TX-Interrupt to them. After the first TETRA box, the RSVP-TE procedure is started to reserve the resources for MS4. Since MS4 is located in the CSwMI, it gets the permission for transmission upon receiving D-TX-Granted from the CSwMI.

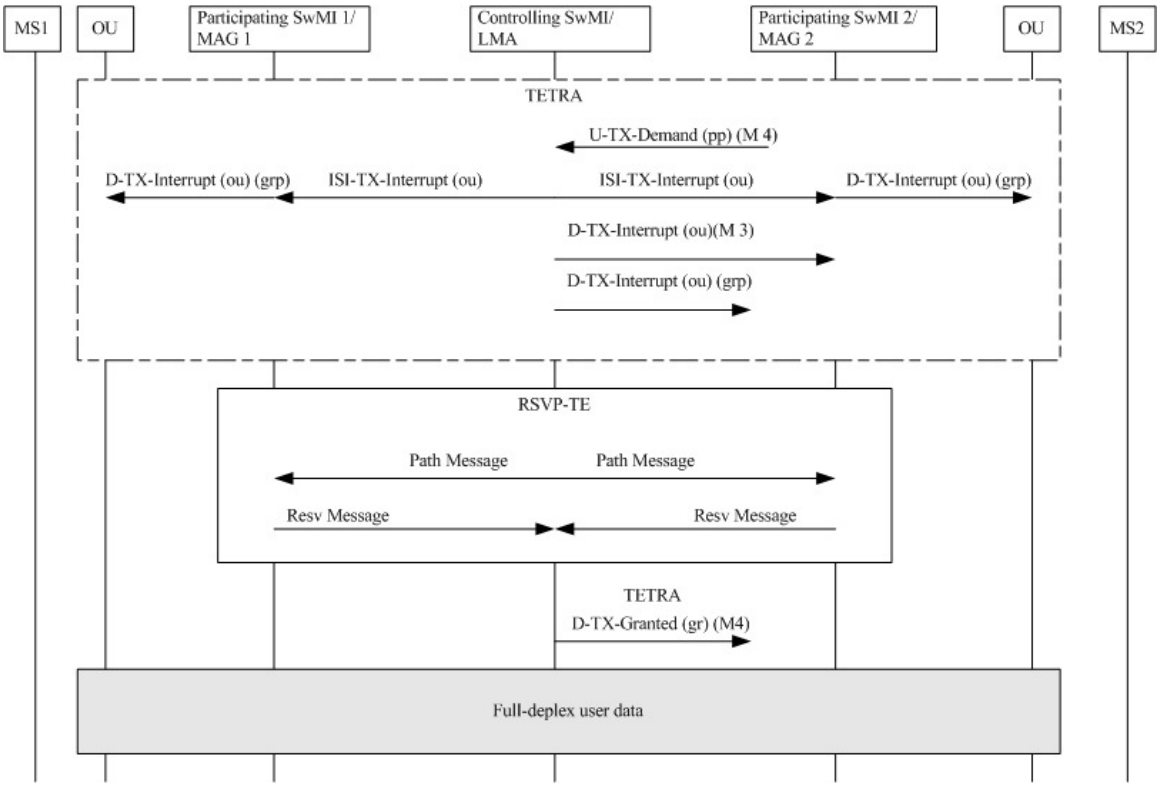

Figure 47: MS4 present at the CSwMI requests to talk at preemptive priority

Figure 48 shows the situation that a MS, i.e., MS4 ceases its transmission.

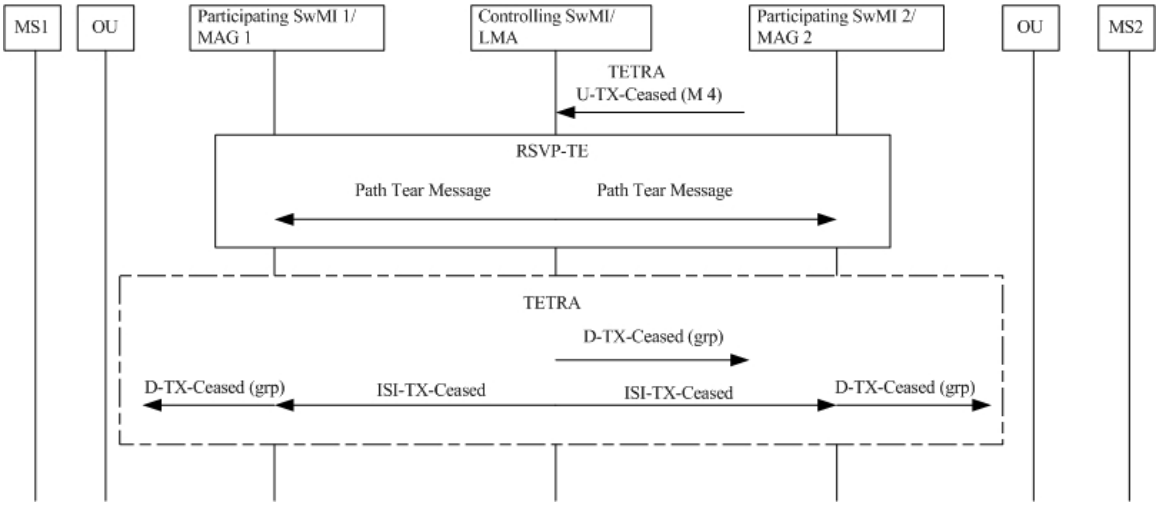

Figure 48: MS4 ceases

Similar to the cease situations that are previously presented, MS4 sends a U-TX-Ceased message to the CSwMI/LMA. Then CSwMI/LMA tears down the LSPs by sending RSVP_PathTear* messages to the PSwMI1/MAG 1 and PSwMI2/MAG 2. In the last

TETRA procedure box, the CSwMI/LMA notifies these two PSwMIs to release their attached users.

4.3.5 Call Handover

Inter-system Handover is a procedure that is needed in situations where a MS is roaming from the coverage area of one wireless access network to the coverage area of another wireless access network. Our core network architecture should be able to support inter-system handover. To perform an inter-system handover, the multicast-enabled Proxy Mobile IP (PMIP) solution is used. When an inter-system handover occurs, the old communication link should be kept such that user data transmission can still continue. In order to show how the inter-system handover signaling procedure is accomplished within the core network, it is needed to combine the call flow of multicast-enabled PMIP, see chapter 3, and the message sequence charts of the call setup scenario where a SwMI joins a connected call, see Section 4.3.2.6. The call flow of multicast-enabled PMIP supports an inter-system multicast handover for a group of users. Actually, depending on which resource allocation policy is used and whether the moving mobile node (MN) is the transmitter or receiver, the inter-system handover for multicast can be divided into two scenarios as follows. Note that in the two scenarios listed below it is assumed that the moving MN is MN2.

1. Handover for multicast when using the permanently allocated resource policy and when the moving MN (MN2) operates as a receiver.
2. Handover for multicast when using the permanently allocated resource policy and when the moving MN (MN2) operates as a transmitter.

We will use message sequence charts to illustrate these two scenarios in the following sections.

4.3.5.1 Handover for multicast when using permanently allocated resource policy and when moving MN is receiver

In this scenario, it is considered that the group attachment is accomplished before the multicast inter-system handover occurs, see Figure 49. In this situation MN2 moves from SWMI / MAG 1 to SWMI / MAG 2.

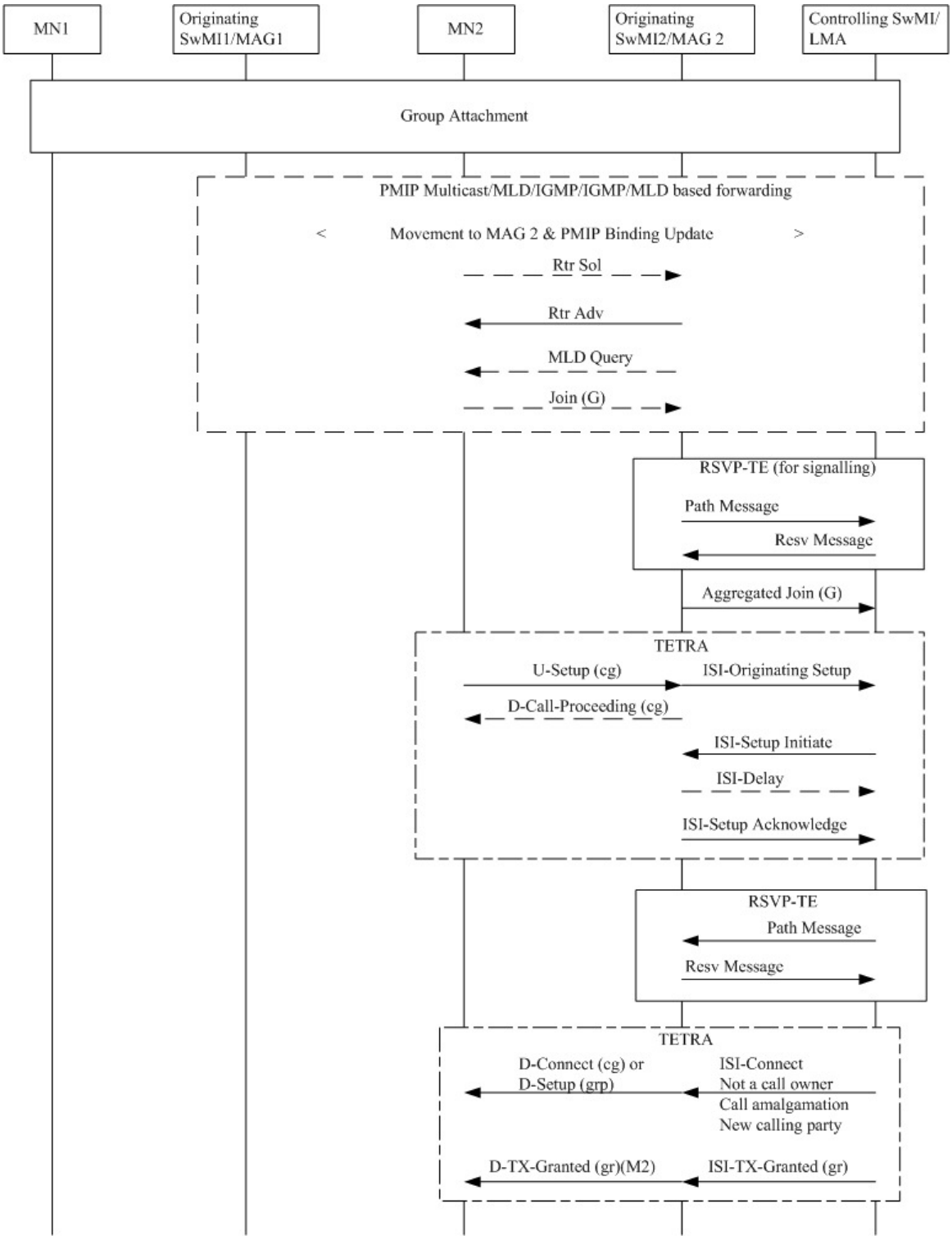

Figure 49: Inter-system handover for multicast when using the permanently allocated resource policy and when moving MN (MN2) is receiver

After MN2 moved to SWMI / MAG 2, the MN2 sends a PMIP Router Solicitation message to SWMI / MAG 2. In response to this, SWMI / MAG 2 sends back a PMIP

Router Advertisement to MN2. Subsequently, SWMI / MAG 2 sends a MLD query to MN2 to learn which multicast addresses are used by listeners. Since MN2 is attached to SWMI / MAG 2, MN2 sends a MLD membership report (Join message) to SWMI / MAG 2. After the PMIP binding update procedures are completed and after SWMI / MAG2 receives the Join message, SWMI / MAG2 starts an RSVP-TE procedure to setup a point-to-point LSP between SWMI / MAG2 and CSWMI / LMA that can be used by the messages belonging to the subsequent signaling procedures between SWMI / MAG2 and CSWMI / LMA. Subsequently, the SWMI / MAG2is triggered to aggregate subscriptions of all mobile nodes that are attached to it by sending an Aggregated Join message to CSWMI / LMA.

Since MN2 operates as a receiver, it will have to start a call setup procedure via MAG2, which is similar to the Scenario described in Section 4.3.2.6.
The RSVP-TE procedures are initiated such that a point-to-point LSP is setup (from CSwMI/LMA towards SwMI/MAG2) and reserved for the user data.
Subsequently, the CSwMI will notify the group and MN2 that the handover is successful.

4.3.5.2 Handover for multicast when using permanently allocated resource policy and when moving MN is transmitter

This inter-system handover scenario is shown in Figure 50. This scenario is similar to the inter-system handover scenario described in Section 4.3.5.1. The only difference is related to the RSVP-TE procedures used to setup and reserve an LSP for the LMA to MAG 2 user data. In this scenario, MN2 is the transmitter. Therefore, this RSVP-TE procedure has to setup LSPs in both directions, CSwMI/LMA to SwMI/MAG2 and SwMI/MAG2 to CSwMI/LMA.

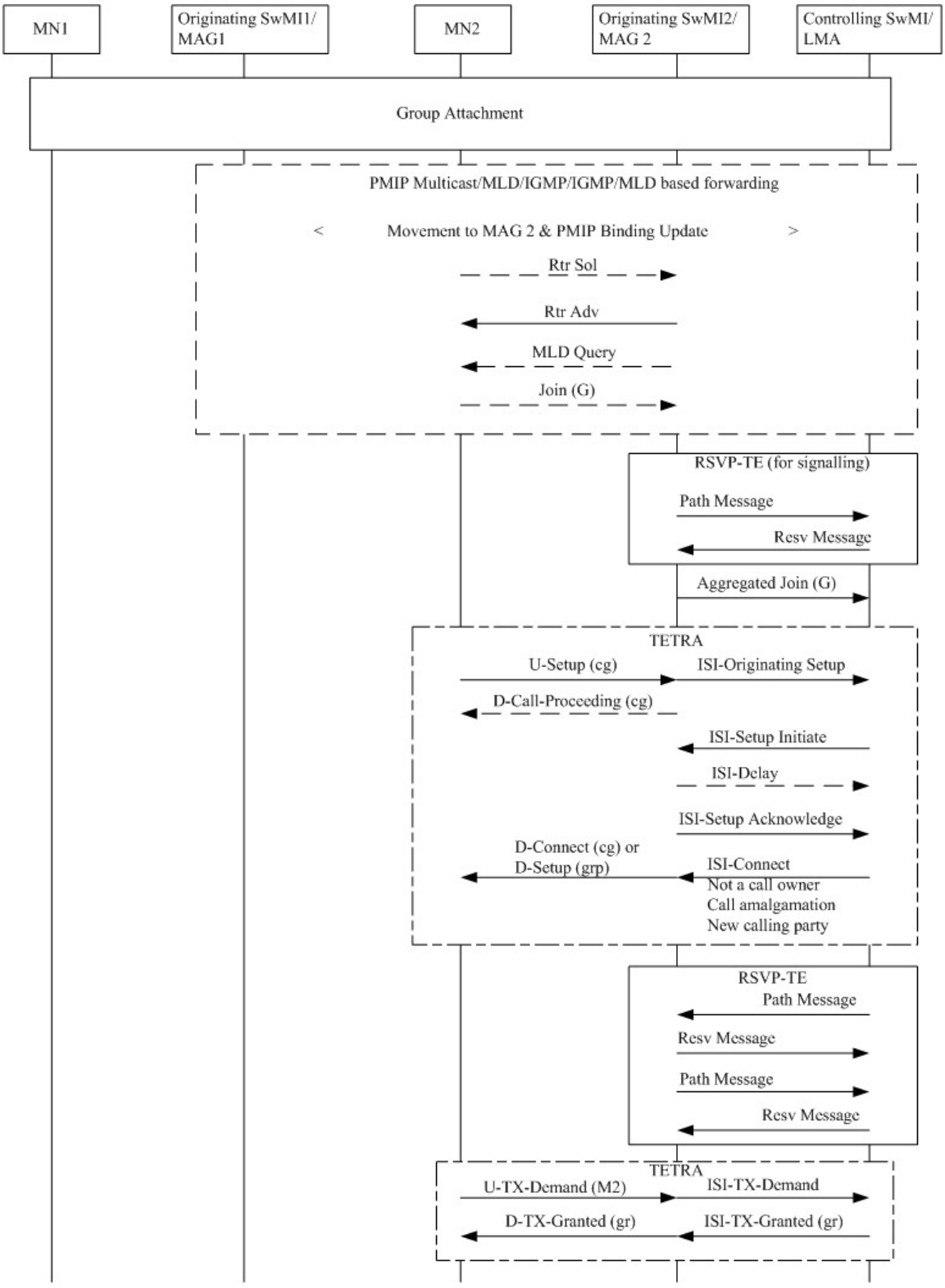

Figure 50: Inter-system handover for multicast when using the permanently allocated resource policy and when moving MN (MN2) is transmitter

4.3.5.3 Unsuccessful Handover Scenarios

In this section, we will show several unsuccessful inter-system handover scenarios.

Figure 51 shows the situation where the inter-system handover scenario described in Section 4.3.5.1 is unsuccessful, due to the fact that the first RSVP-TE procedure shown in Figure 49 is unsuccessful. In this case an RSVP_PathErr message is sent by CSwMI/LMA towards the SwMI/MAG2, see Figure 51. Due to this situation the SwMI/MAG 2 does not send the aggregated join towards CSwMI/LMA.

.

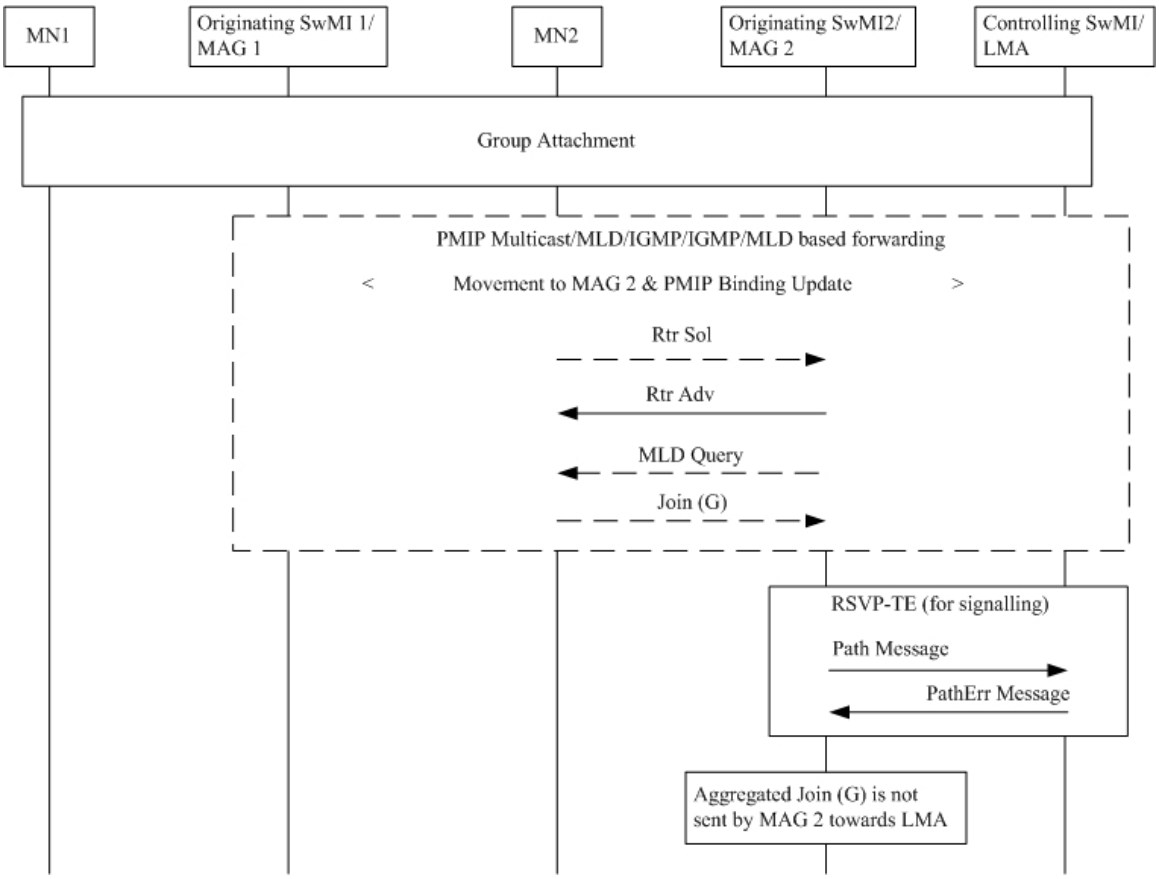

Figure 51: Unsuccessful inter-system handover scenario: first RSVP-TE procedure is unsuccessful

Figure 52 shows the situation where the inter-system handover scenario described in Section 4.3.5.1 is unsuccessful, due to the fact that the *aggregated join* message is not accepted by the CSwMI/LMA.

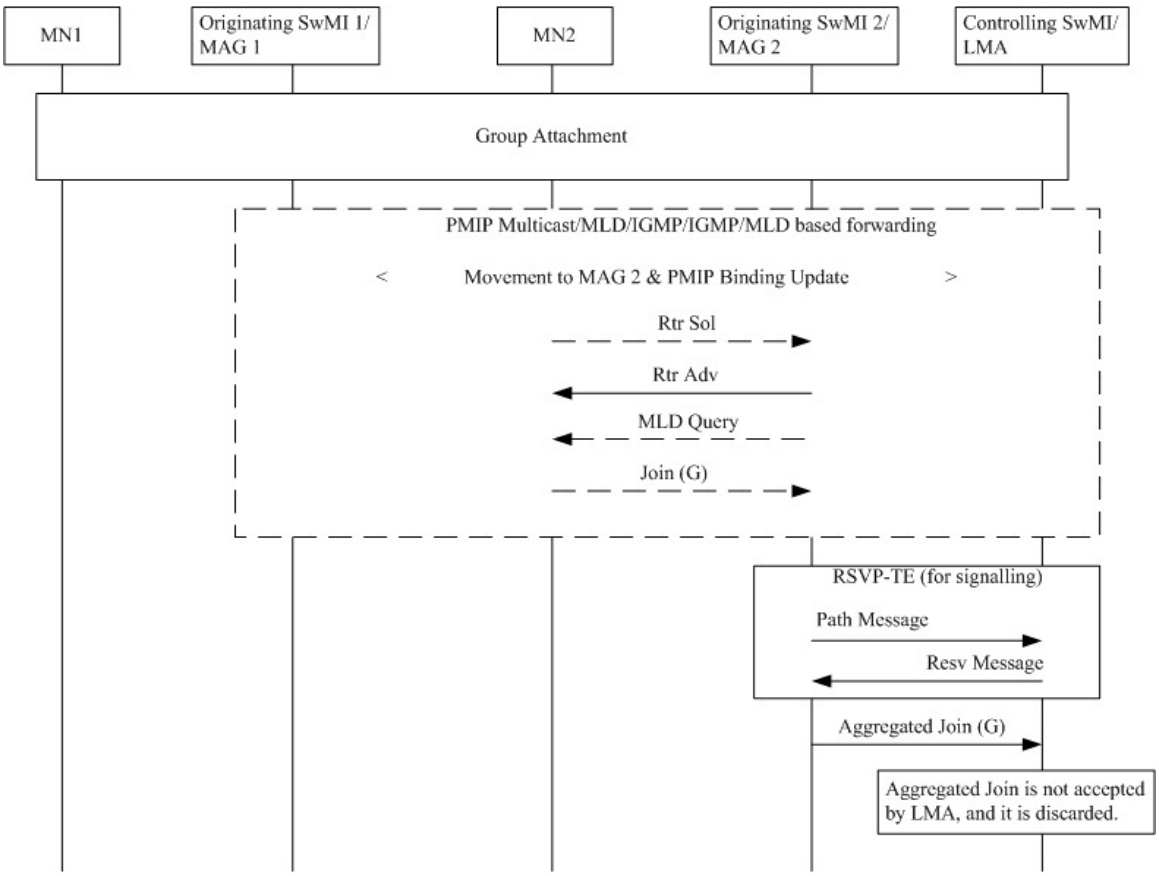

Figure 52: Unsuccessful inter-system handover scenario: Aggregated join is not accepted

Figure 52 shows the situation where the inter-system handover scenario described in Section 4.3.5.1 is unsuccessful, due to the fact that the second RSVP-TE procedure shown in Figure 49 is unsuccessful. In this case an RSVP_PathErr message is sent by CSwMI/LMA towards the SwMI/MAG2, see Figure 52. Due to this situation no LSPs are setup between the SwMI/MAG 2 and LMA. Subsequently, MN2 is notified that the inter-system handover is unsuccessful.

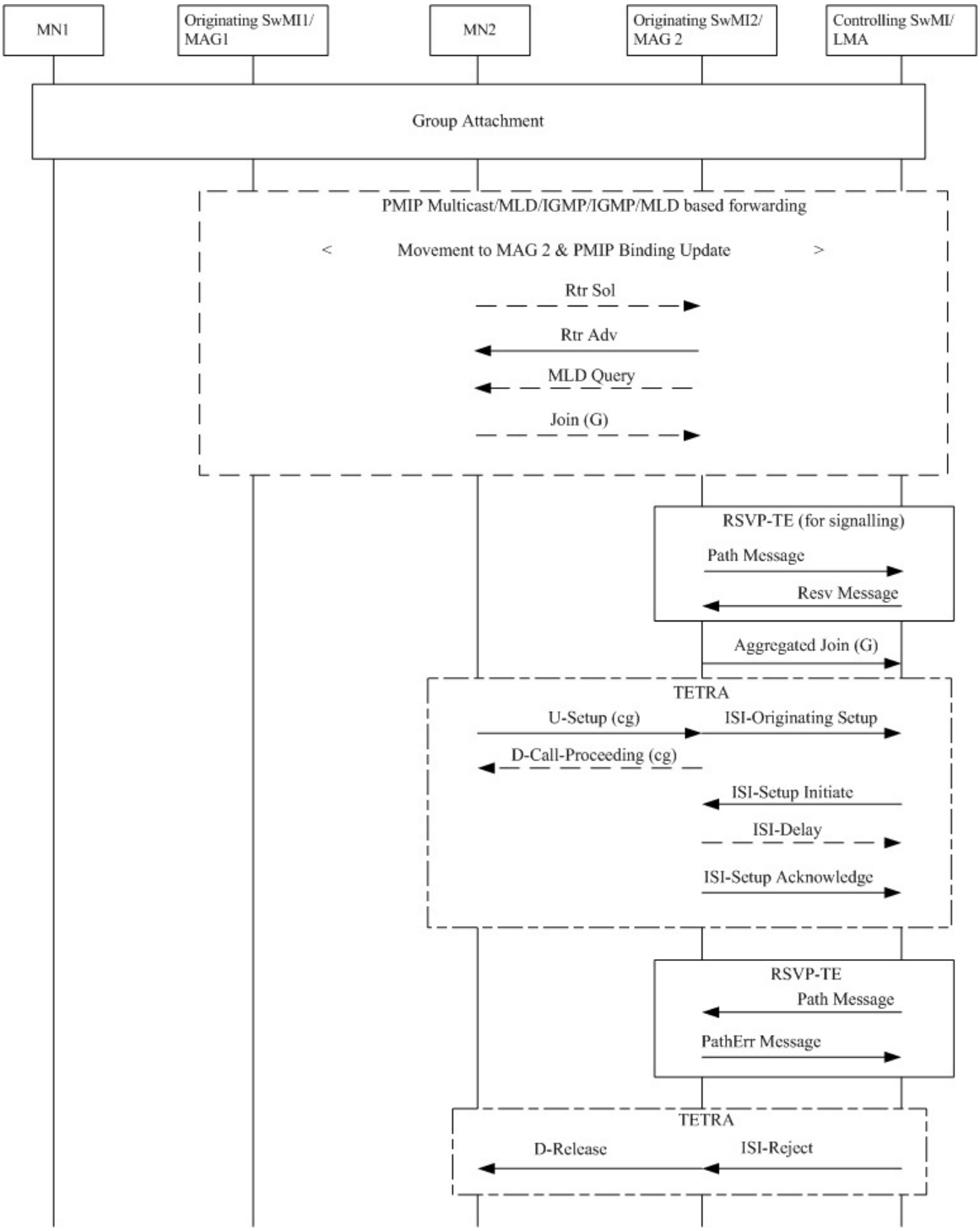

Figure 53: Unsuccessful inter-system handover scenario: second RSVP-TE procedure is unsuccessful

4.3.6 Group Leave

Group leave is a procedure that is used in the situation that one or more group members leave the group. Two group leave cases can be distinguished: 1. Individual members leave the group call. 2. All group members leave the group call.

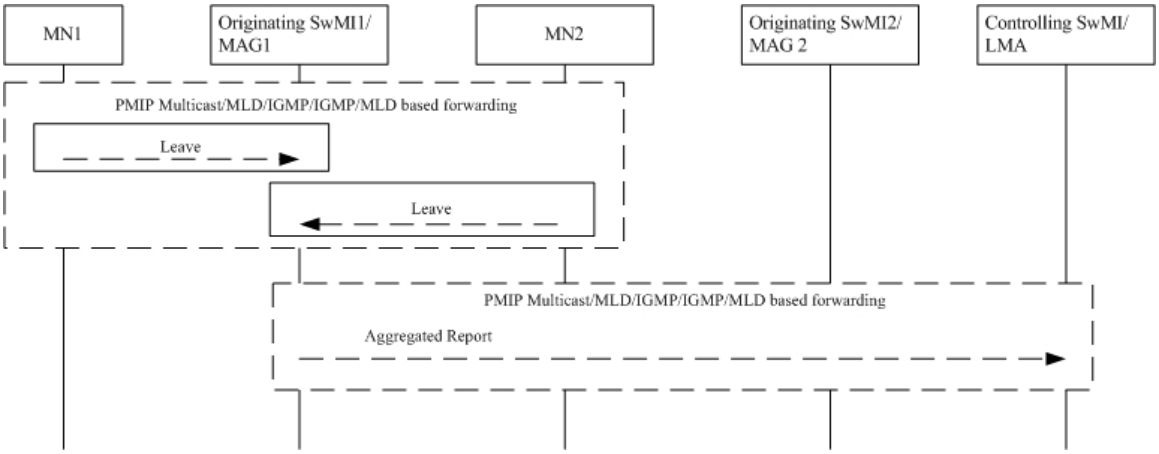

Figure 54: Individual members leave the group call

An example that depicts the first case is shown in Figure 54, where MN1 and MN2 want to leave the group. Both MNs send leave message to the OSwMI1/MAG 1 where they are attached to. Then aggregated report is sent to the CSwMI/LMA to remove the two MNs from the multicast address associated with OSwMI1/MAG 1.

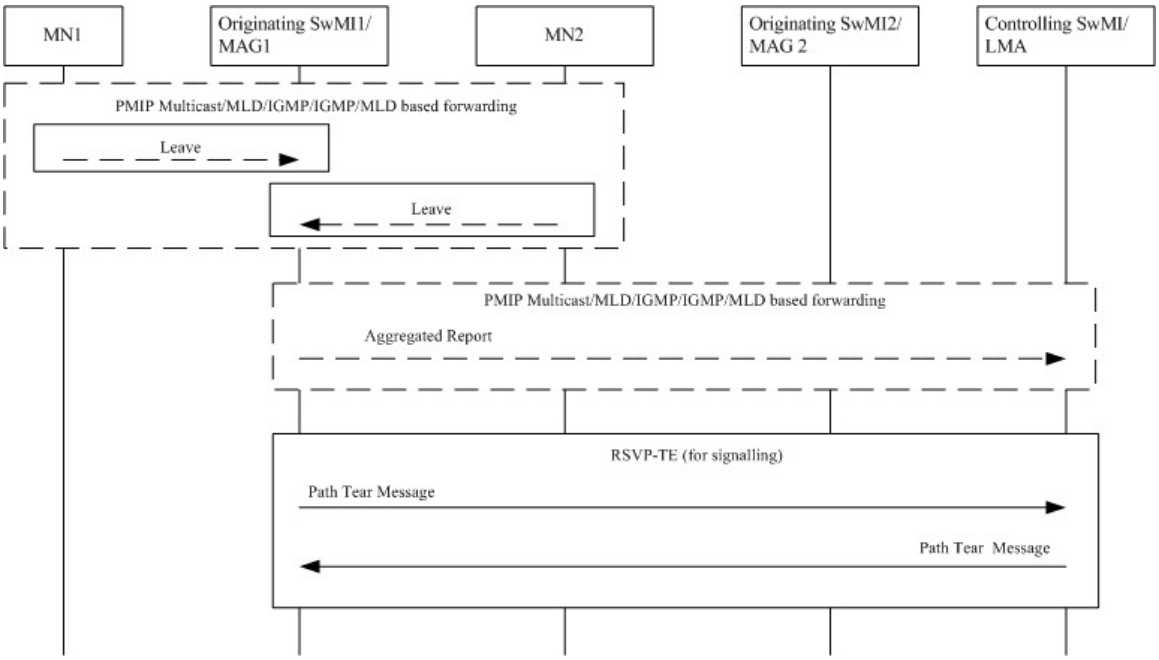

Figure 55: All group members attached to SwMI1/MAG1 leave the group

An example that depicts the second case is shown in Figure 55, where all the group members attached to SwMI1 / MAG1 need to leave the group. In this case the LSPs associated with this group (attached to SwMI1 / MAG1) will have to be released. This is accomplished by using an RSVP-TE release procedure, see Figure 55.

4.3.7 Call Release

4.3.7.1 The release of a SwMI from a call

In this scenario, see Figure 56, one of the SwMI/MAGs is released from a call. Actually, in this case the call is not completely terminated. Only the PSwMI2/MAG 2 is released from a call. So the resources along the LSP that is between the CSwMI/LMA and the PSwMI2/MAG 2 is released by using a Path Tear message. Although PSwMI 2/MAG 2 is released, the CSwMI may continue with the call since PSwMI1/MAG 1 is not released.

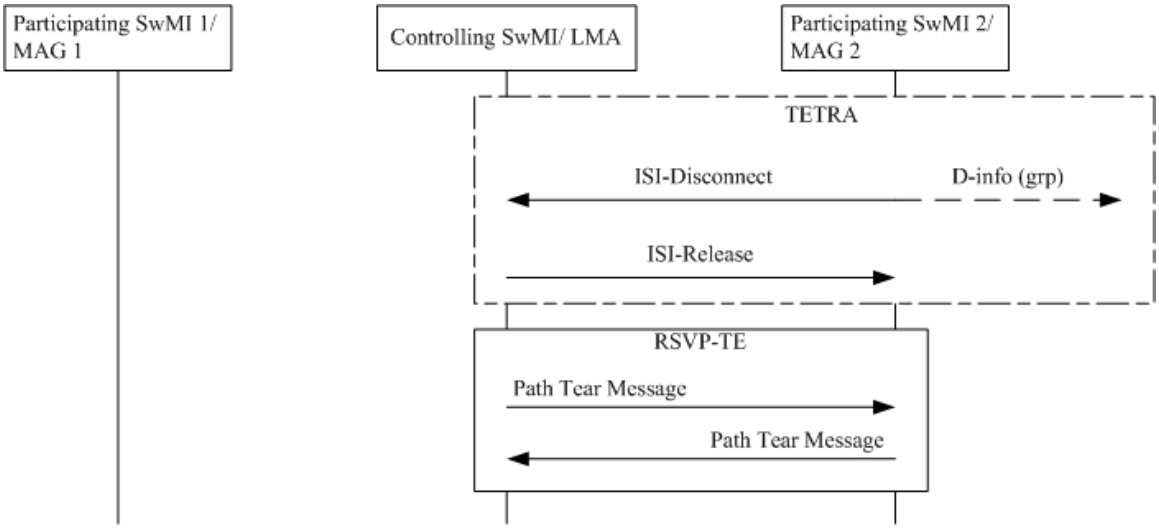

Figure 56: The release of a PSwMI from a call

4.3.7.2 Call disconnection, as a result of calling party disconnecting

When a call is completed then it has to be terminated. The common way to do this is that calling party disconnects the call. This call release scenario is shown in Figure 57. In this case the CSwMI/LMA starts releasing the call after it receives the U-Disconnect message from the calling MN. When a call is finished, the calling party sends U-Disconnect to the OSwMI1/ MAG 1. This message triggers OSwMI/MAG to send ISI-Disconnect to the CSwMI/LMA. Then the CSwMI/LMA releases the call by sending ISI-Release to the OSwMI/MAG and PSwMI/MAG. After sending ISI-Release messages, the CSwMI/LMA starts RSVP-TE procedures to tear down the available LSPs. The second TETRA procedure box shows that the D-Release message is sent to the group members that are

attached to the Originating SwMI/MAG and Participating SwMI/MAG, such that the group call is released.

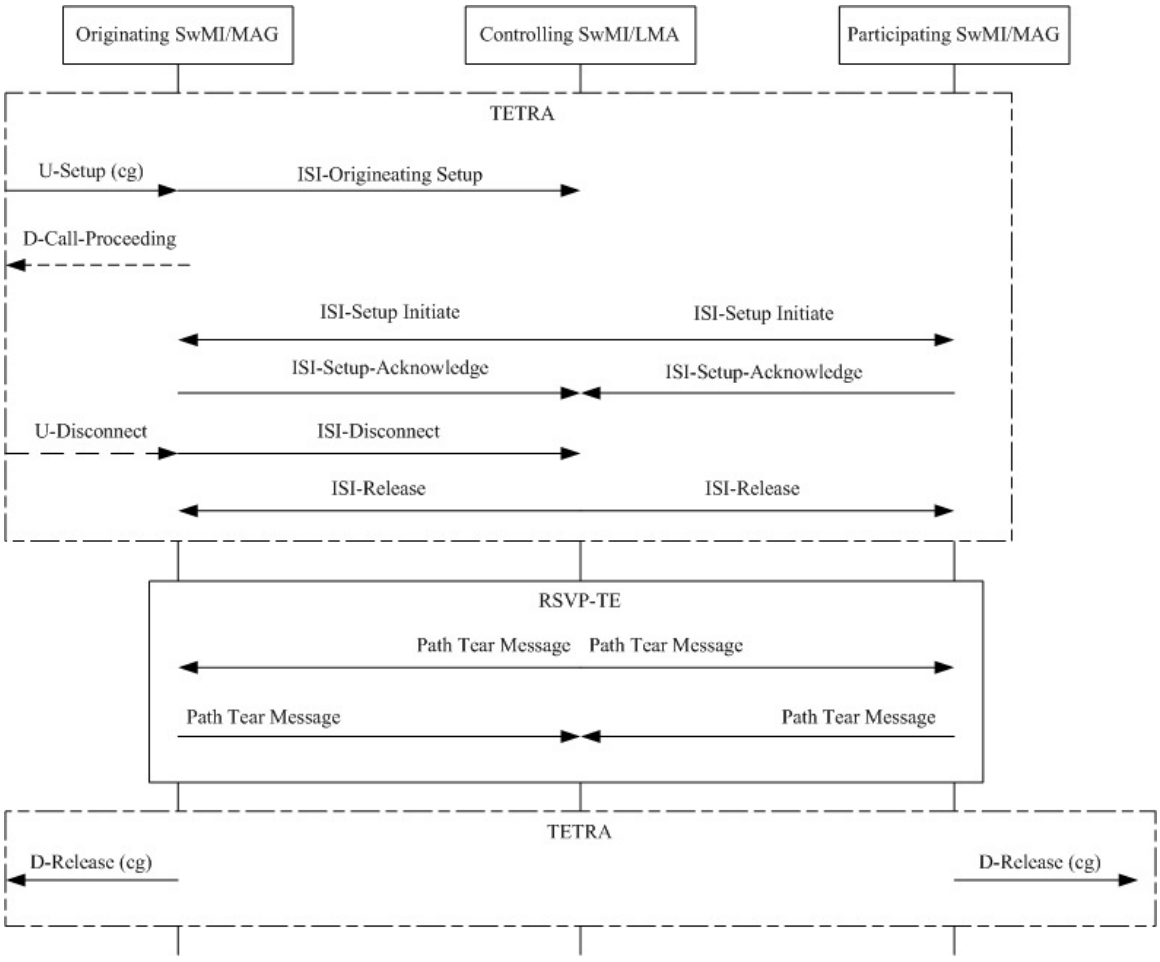

Figure 57: Call disconnection, as a result of calling party disconnecting

4.3.7.3 Call disconnection, as a result of a PSwMI disconnecting

In this call release scenario, a PSwMI disconnects the call. In Figure 58 the PSwMI1/MAG 1 initiates the disconnection of a call by sending an ISI-Disconnect message to the CSwMI/LMA. Then the CSwMI/LMA sends an ISI-Release message to the PSwMI2/MAG 2. Afterwards, the RSVP-TE starts to tear down the LSPs available between the CSwMI/LMA and the PSwMI2/MAG 2 so that the resources can be released. After this step, D-Release messages are sent to the group members that are attached to the PSwMI2/MAG 2. Similarly, CSwMI/LMA also sends D-Release to the attached group members. As we have two PSwMIs in this case, the CSwMI/LMA also sends ISI-Release to the PSwMI1/MAG 1. Afterwards, the RSVP-TE starts to tear down the LSPs between the CSwMI/LMA and the PSwMI1/MAG 1 to release the resources along this LSP. After the second RSVP-TE procedure box, PSwMI1/MAG 1 releases the group members that belong to it by sending D-Release to them. Now the call is completely released.

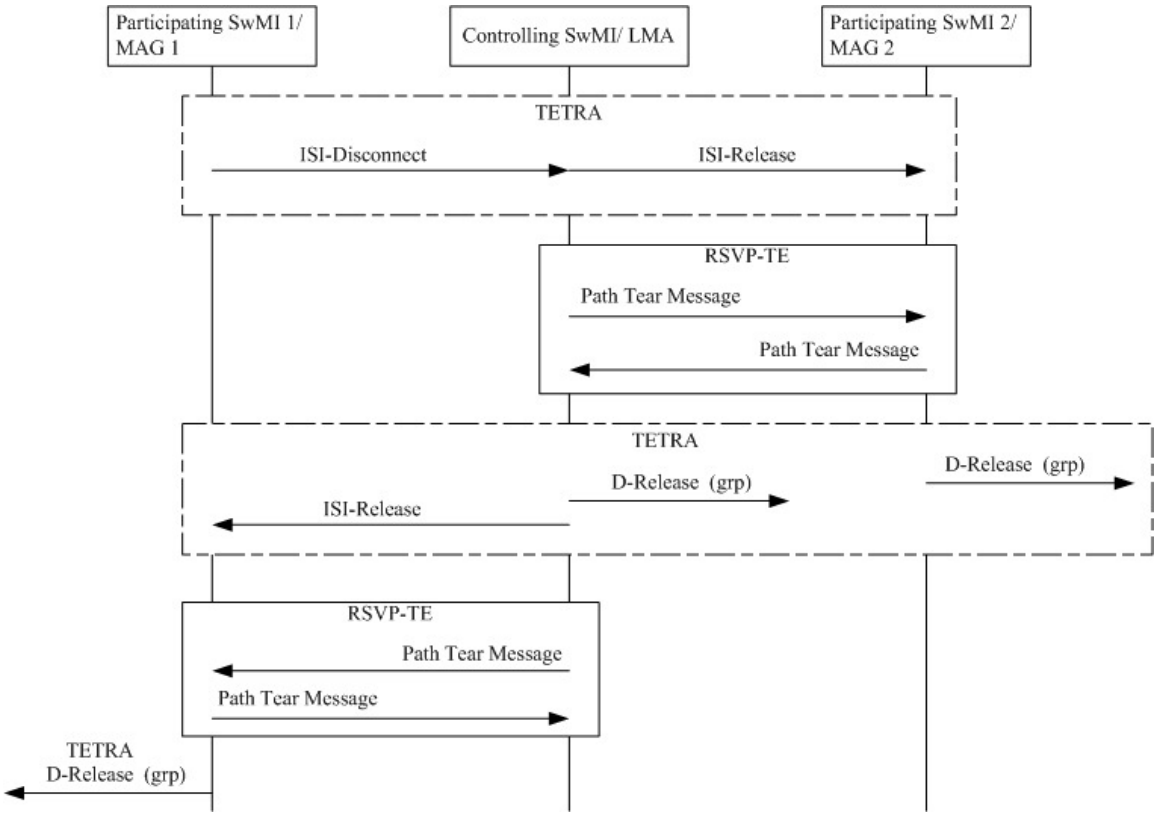

Figure 58: Call disconnection, as a result of a PSwMI disconnecting

4.3.7.4 Call disconnection by the CSwMI

In this call release case, the CSwMI/LMA terminates a group call. This call release case is quite straightforward. To close down the call, the CSwMI/LMA sends ISI-Release messages to all the involved SwMIs, see Figure 59.

After the ISI-Release messages have been sent, an RSVP-TE release procedure is started by the CSwMI/LMA to release all the LSPs towards all SwMI/MAGs. Once this procedure is done, group members receive D-Release messages from two the SwMIs. Therefore, all the members are released and the call is terminated.

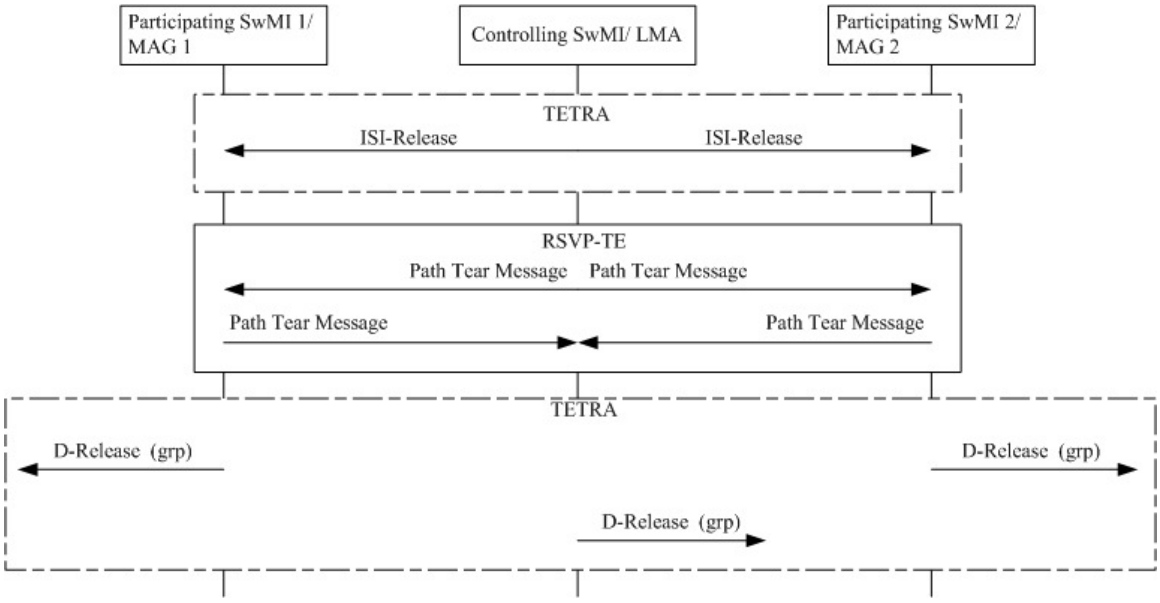

Figure 59: Call disconnected by the CSwMI

Chapter 5: Architecture Evaluation

The core network architecture that is described in Chapter 4 is targeted to interconnect various heterogeneous wireless communication systems. Scalability can be considered as a critical performance measure since the number of wireless access networks may increase significantly. Therefore, this chapter describes the evaluation of the core network architecture with respect to scalability.

In order to analyze the scalability of the core network architecture the message sequence charts used by the various core network features have to be applied. However, due to the fact that the core network architecture supports a large number of such features, it is required to select a limited number of such features. To do this, only the most significant features are selected. These are: (1) Group establishment, (2) Group call setup, (3) Push to talk, (4) Group call release, (5) Group call handover, (6) Group leave.
Scalability is measured by calculating the number of signaling messages (i.e., signaling load) per selected signaling procedure when the number of wireless access networks supported by the core network is increased. In order to calculate the number of signaling messages analytical formulas are derived.

The message sequence charts that are used for the calculation of the number of signaling messages per signaling procedure are described in Chapter 4. For reasons of clarity we copy the relevant message sequence chart figures from Chapter 4 and also show them in this chapter.

5.1 Signaling Load for Group Establishment

The message sequence chart for group establishment is described in Section 4.3.1. This message sequence chart is also depicted in Figure 60. Based on the group establishment message sequence chart presented in Figure 60 it can be seen that two MAGs are used in this group attachment scenario. Two mobile users are attached to MAG 1.

The number of RSVP_Path messages is equal to 2 times the number of MAGs that are supporting users that are willing to join a certain group. The same holds for the RSVP_Resv message. The number of MLD Aggregated Join messages is one times the number of MAGs that are supporting users that are willing to join a certain group.

For each wireless access network one MAG is used. Thus the number of MAGs (N) is identical to the number of wireless access networks.
Based on the above we derive the following equations:

- Number of RSVP_Path message=2*N (Eq. 5.1)
- Number of Resv message=2*N (Eq. 5.2)
- Number of MLD Aggregated Join=1*N (Eq. 5.3)

Where N represents total number of wireless access networks.

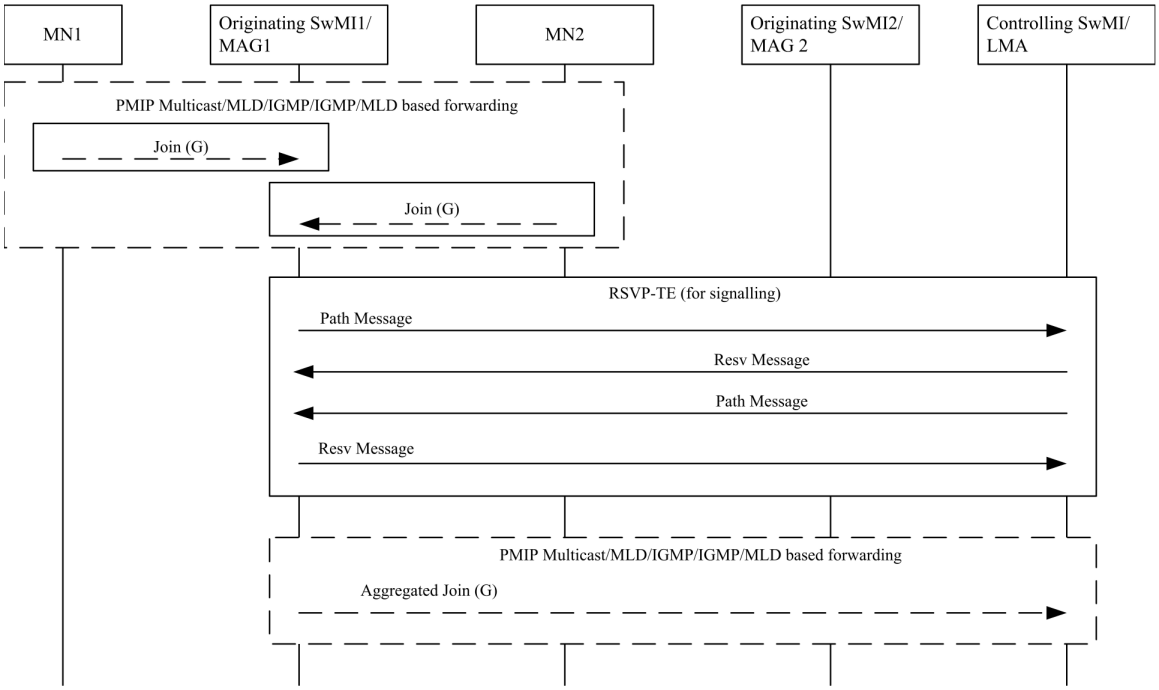

Figure 60: Group attachment

In Figure 61 the number of signaling messages versus the number of wireless access networks used for Group establishment is shown.

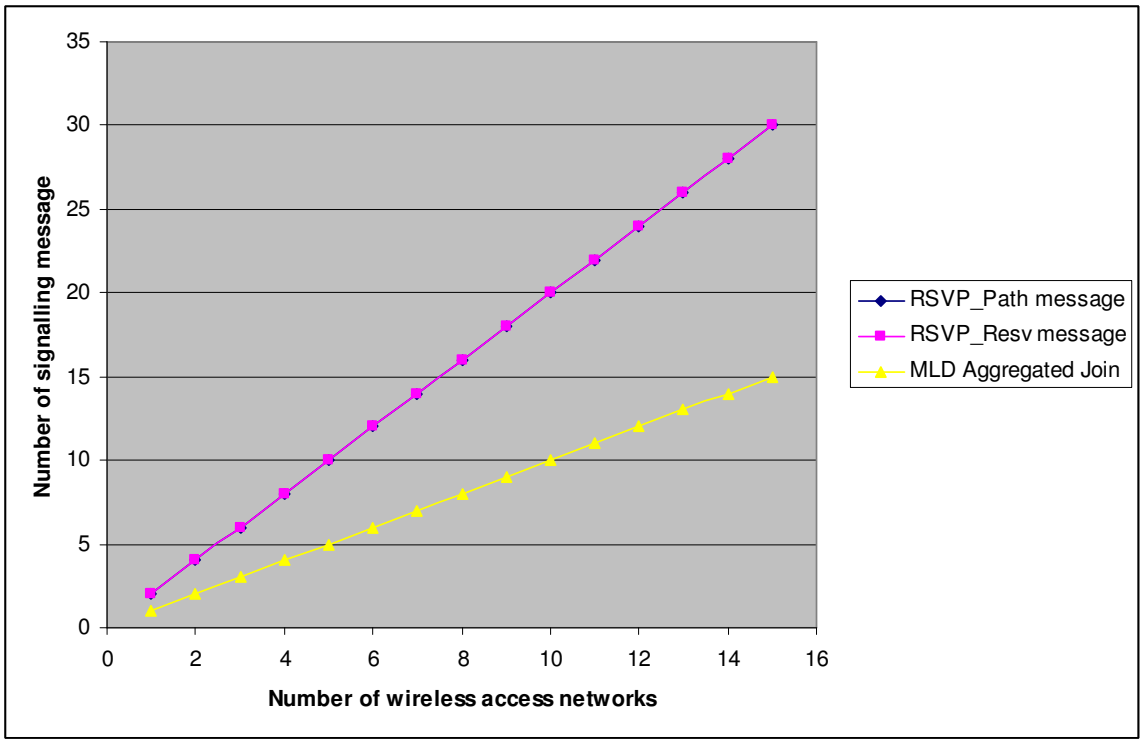

Figure 61: Signaling load vs wireless access networks used for Group establishment

Based on Figure 61, it can be concluded that when the number of wireless access networks is increasing, the number of RSVP_Path messages, RSVP_Resv messages and MLD Aggregated Join messages increase linearly (see Eq. 5.1, Eq. 5.2, Eq. 5.3, respectively).

5.2 Signaling Load for Group Call Setup

In this section, we choose two call setup scenarios to calculate the signaling load: One of them is the group call setup with single calling party and no queuing for resources, see Section 4.3.2.1. The other one is the scenario that is similar to the previous mentioned scenario with the difference that now the RSVP-TE sets up and reserves multipoint-to-multipoint LSPs within the core network.

Figure 62 shows the message sequence chart associated with the first group call scenario.

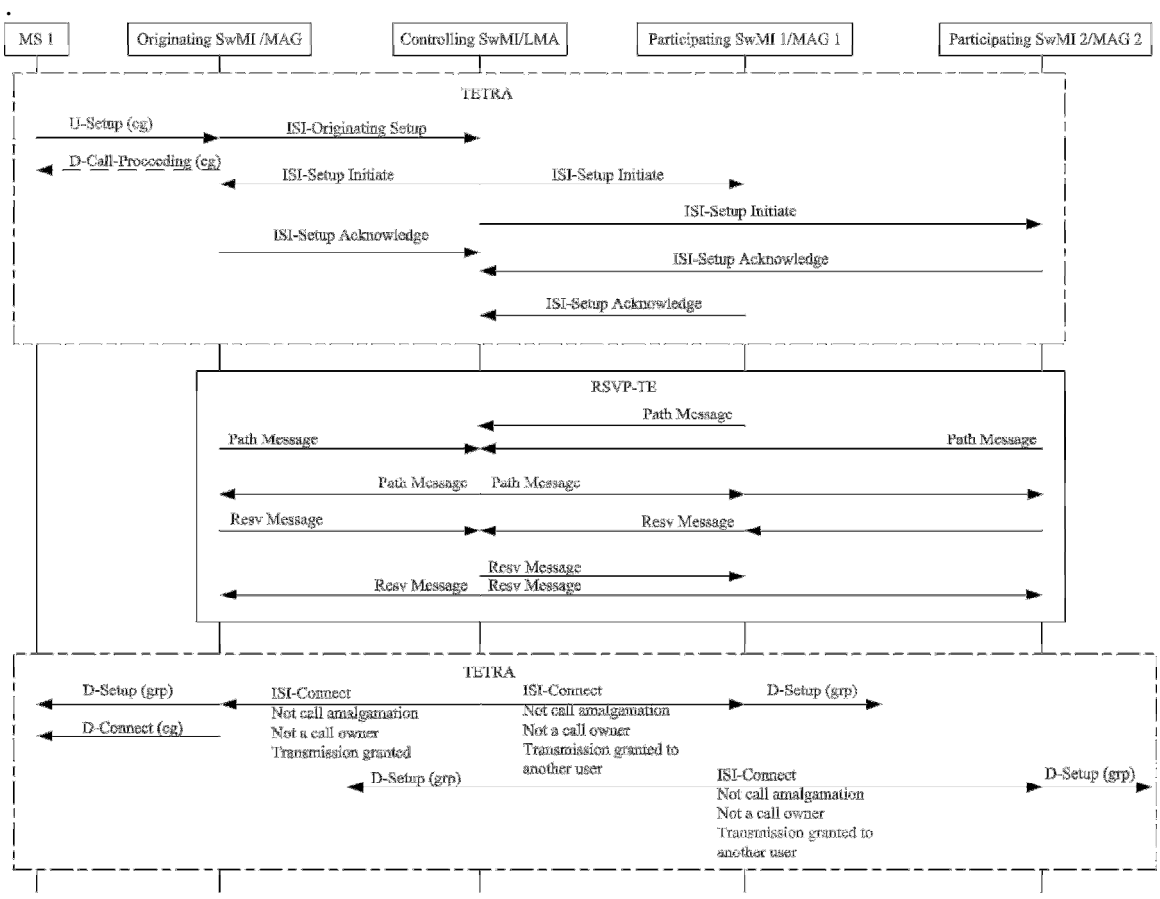

Figure 62: Single calling party, no queuing for resources

Regarding the scenario where only one point-to-multipoint LSP is set up from the CSwMI / LMA towards the SwMI / MAGs we derived the following.

It is important to note that in order to calculate the number of RSVP-TE messages that is shown in Figure 62, a number of assumptions is used.

It is assumed that only one point-to-multipoint LSP is setup between the CSwMI towards the SwMIs/MAGs. This will mean that two or more MAGs cannot send user data towards the core network simultaneously.
A general equation that could be used to calculate the RSVP signaling load is given below:

Number of RSVP-TE signaling messages = N*(1*RSVP_Path+1*RSVP_Resv) + (1→N)*(1*RSVP_Path+1*RSVP_Resv)

In this equation, N represents the number of the wireless access networks. 1→N represents the situation that LMA needs to set up point to multipoint LSPs between the LMA and N MAGs in order to multicast information from the LMA towards N MAGs. Due to the fact that the RSVP messages are sent on a point-to-multipoint manner between LMA and

MAGS, we consider that for one communication path between LMA and N MAGS, N*(m+1)*RSVP messages are sent. The m value depends on the number of interior routers located on the point-to-multipoint communication paths found by the used routing protocol.

The number of RSVP_Path messages is equal to (2*(m+1)) N.

For this scenario equations are derived for the number of RSVP_Path, RSVP_Resv and TETRA ISI messages.

The number of TETRA ISI-Originating Setup is one since only one mobile user only needs to send one ISI-Originating Setup to the LMA regardless the involved MAGs. The numbers of other TETRA ISI messages are 1*N. So we use the following equations to calculate the number of signaling messages:

Number of RSVP_Path message==2*N (Eq. 5.4)
Number of RSVP_Resv message=2*N (Eq. 5.5)
Number of TETRA ISI-Setup Initiate=1*N (Eq. 5.6)
Number of TETRA ISI-Setup Acknowledge=1*N (Eq. 5.7)
Number of TETRA ISI-Connect=1*N (Eq. 5.8)
Number of TETRA ISI-Originating Setup=1 (Eq. 5.9)

Please note that in Eq. 5.4 and Eq. 5.5 it is considered that the value of the parameter m = 0. The signaling load that is derived using Eq. 5.4 to Eq. 5.9 is depicted Figure 63.

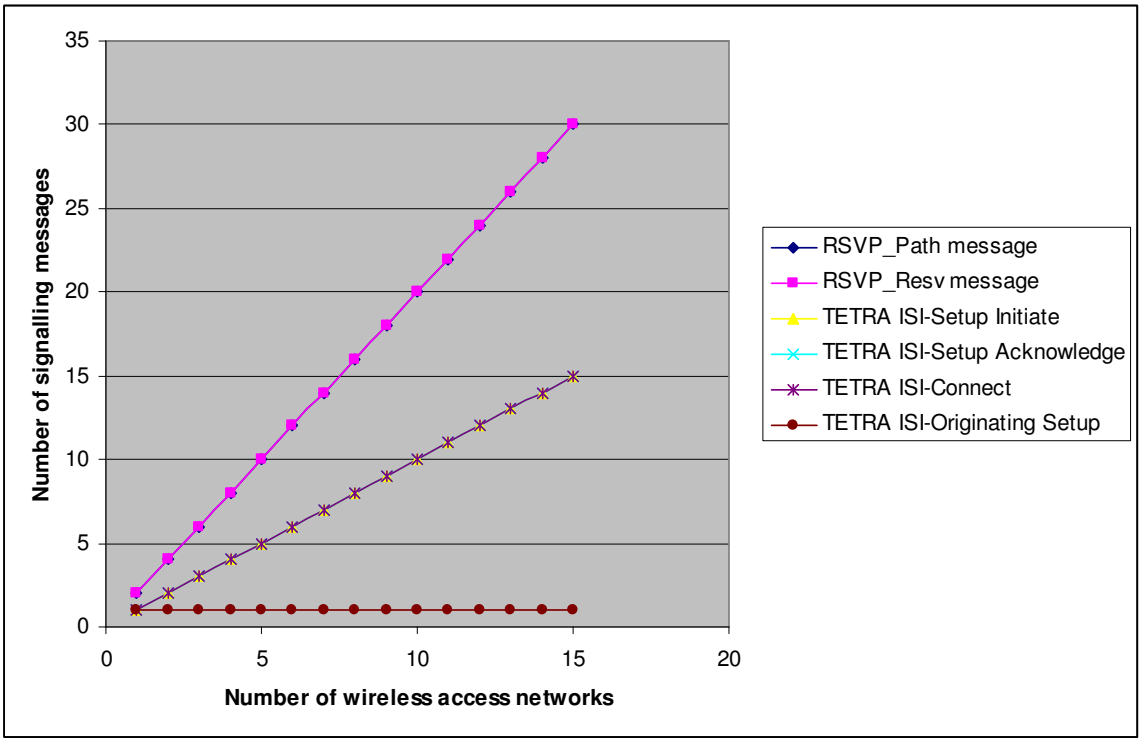

Figure 63: Signaling load vs. wireless access networks for call setup, single calling party, no queuing for resources, when one point-to-multipoint LSP is set up

As can be seen from Figure 63, when N increases, both the number of RSVP_Path and number of RSVP_Resv messages increase linearly. All the TETRA ISI messages increase linearly except the TETRA ISI-Originating Setup, which is constant (=1) regardless the number of the wireless access networks.

Regarding the scenario where only multipoint-to-multipoint LSPs are set up from the CSwMI / LMA towards and from the SwMI / MAGs we derived the following. This will mean that two or more MAGS can send user data towards the core network simultaneously.

The previous presented equations then become:

Number of RSVP-TE signaling message=N (RSVP_Path+ RSVP_Resv) + N*(N* RSVP_Path+N* RSVP_Resv) =N (RSVP_Path+ RSVP_Resv) +N^2 (RSVP_Path+ RSVP_Resv). The numbers of TETRA ISI messages are the same as in the ones given in the previous presented scenario. So the following equations can be derived:

Number of RSVP_Path message=N+ N^2 (Eq. 5.10)
Number of RSVP_Resv message=N+ N^2 (Eq. 5.11)
Number of TETRA ISI-Setup Initiate=1*N (Eq. 5.12)
Number of TETRA ISI-Setup Acknowledge=1*N (Eq. 5.13)
Number of TETRA ISI-Connect=1*N (Eq. 5.14)
Number of TETRA ISI-Originating Setup=1 (Eq. 5.15)

Based on these equations, we generate Figure 64.

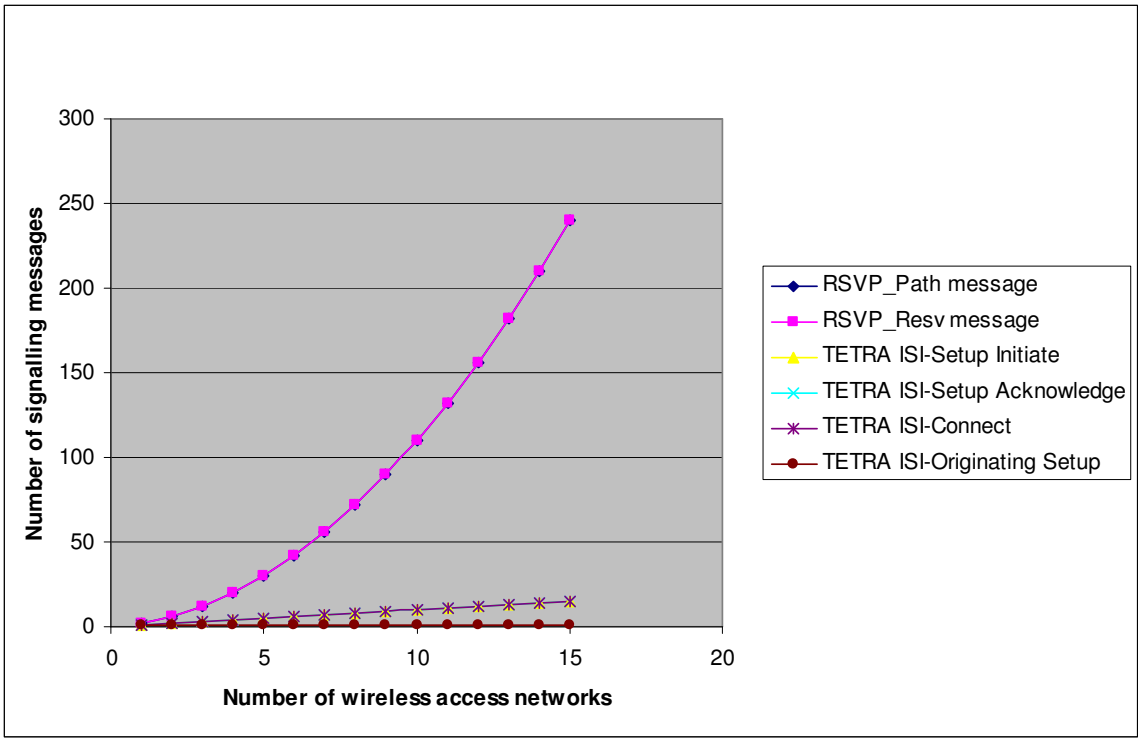

Figure 64: Signaling load vs. wireless access networks for call setup, single calling party, no queuing for resources, when one multipoint-to-multipoint LSPs are set up

From Figure 64 it can be seen that when N increases the numbers of RSVP_Path message and RSVP_Resv message both increase exponentially due to the factor N^2 in Eq. 5.10 and Eq. 5.11, respectively. The number of the TETRA ISI messages is equal to the ones given in Figure 64.

5.3 Signaling Load for Push to Talk

As it has been discussed in chapter 4, four different scenarios can be distinguished for achieving the push to talk procedure:

1. Normal way for PTT when using the permanently allocated resources policy;
2. ODINI way for PTT when using the permanently allocated resources policy;
3. Normal way for PTT when using the temporary allocated resources policy;
4. ODINI way for PTT when using the temporary allocated resources policy.

This section will derive and depict the signaling load associated with these four push to talk scenarios.

5.3.1 Signaling load for PTT Normal way when using permanently allocated resources policy

The message sequence chart for this PTT scenario is already given in Section 4.3.3.1. This message sequence chart is also copied in Figure 65.

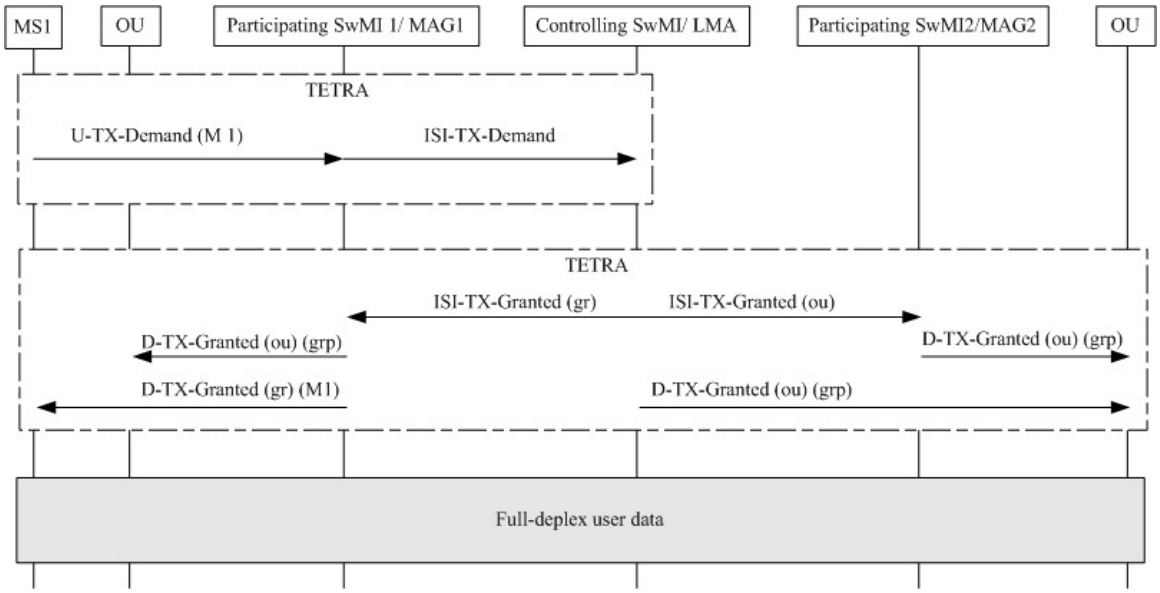

Figure 65: PTT *normal way* when using permanently allocated resources policy

Based on this message sequence chart, we derived that only one TETRA ISI-TX-Demand independently on the number wireless access networks. Moreover, the number of TETRA ISI-TX-Granted depends on the number of wireless access networks (MAGs). So we derive the following equations:

Number of TETRA ISI-TX-Demand=1 (Eq. 5.16)
Number of TETRA ISI-TX-Granted=1*N (Eq. 5.17)

Again N represents the number of wireless access networks (or the number of MAGs). Figure 66 depicts the signaling load vs the number of wireless access networks active in a PTT procedure. This graph is derived using Eq. 5.16 and Eq. 5.17.

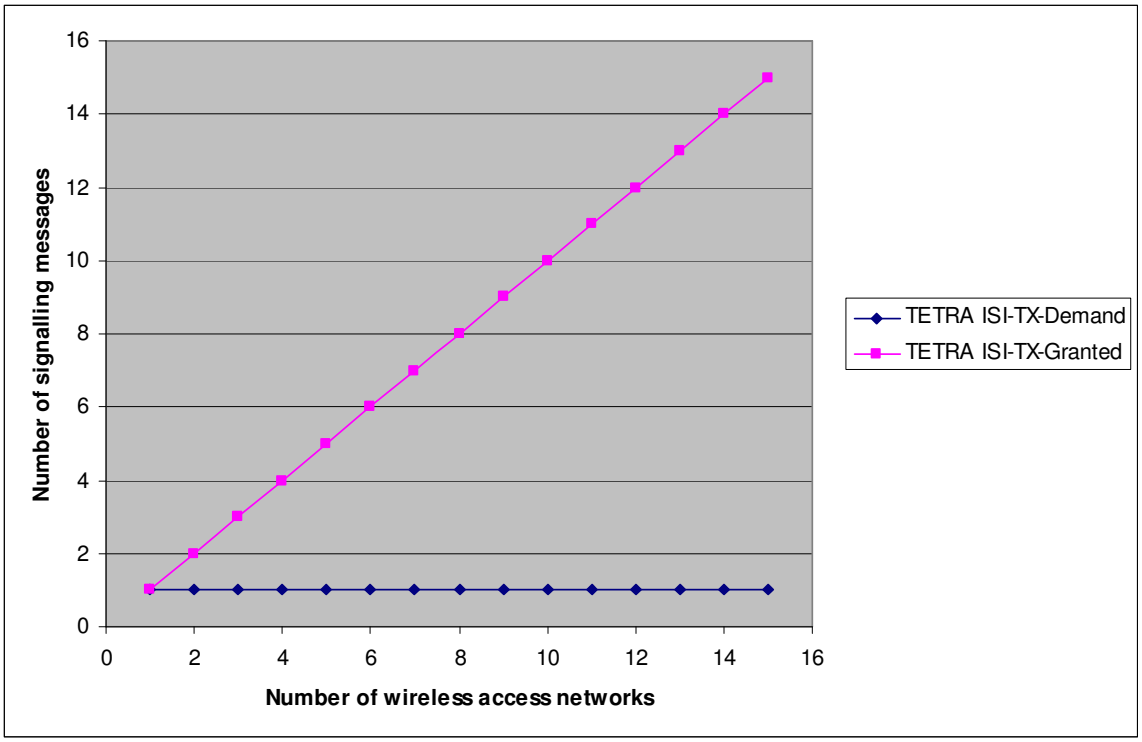

Figure 66: Signaling load vs. wireless access networks for PTT *normal way* when using permanently allocated resources policy

As can be seen from Figure 66 the number of TETRA ISI-TX-Granted signaling messages increases linearly when the number of wireless access networks is increased. The number of TETRA ISI-TX-Demand remains equal to 1.

5.3.2 Signaling load for PTT ODINI way when using permanently allocated resources policy

The message sequence chart for this PTT scenario is already given in Section 4.3.3.2. This message sequence chart is also copied in Figure 67.

The message sequence chart given in Figure 67 is used to calculate the signaling load of this PTT scenario. The derived equations are given below. It is important to see that the derived equations for this PTT scenario are the same as the ones derived for the PTT normal way scenario described in Section 5.3.1.

Number of TETRA ISI-TX-Demand=1 (Eq. 5.17)
Number of TETRA ISI-TX-Granted=1*N (Eq. 5.18)

This means that the signaling load vs wireless access networks graphs related to this procedure see Figure 68, are identical to the ones given in Figure 66.

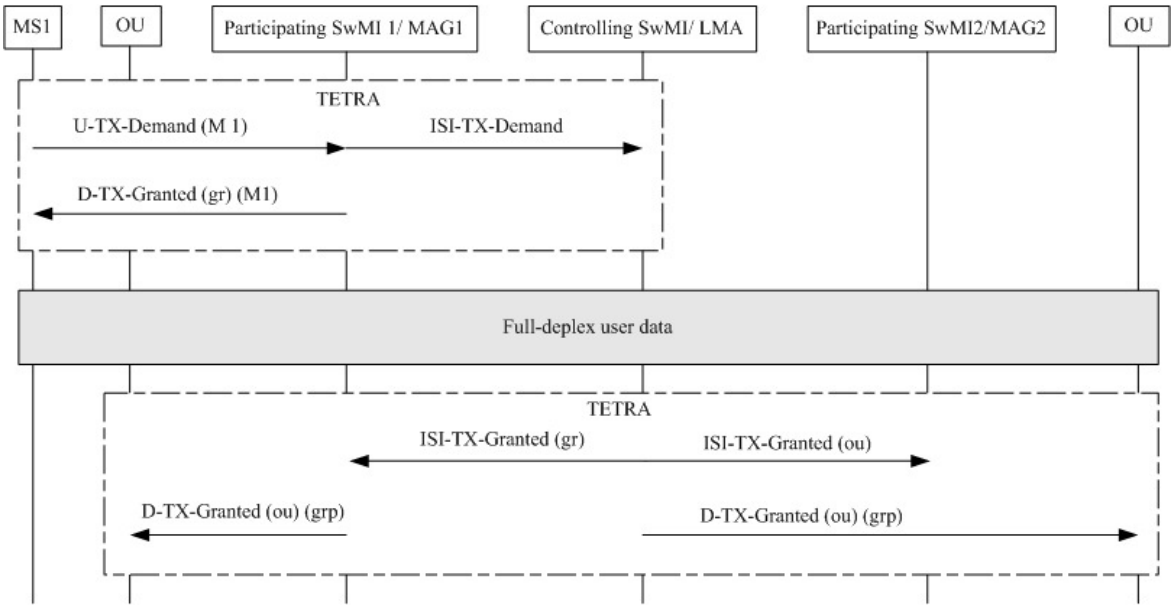

Figure 67: PTT *ODINI way* when using permanently allocated resources policy

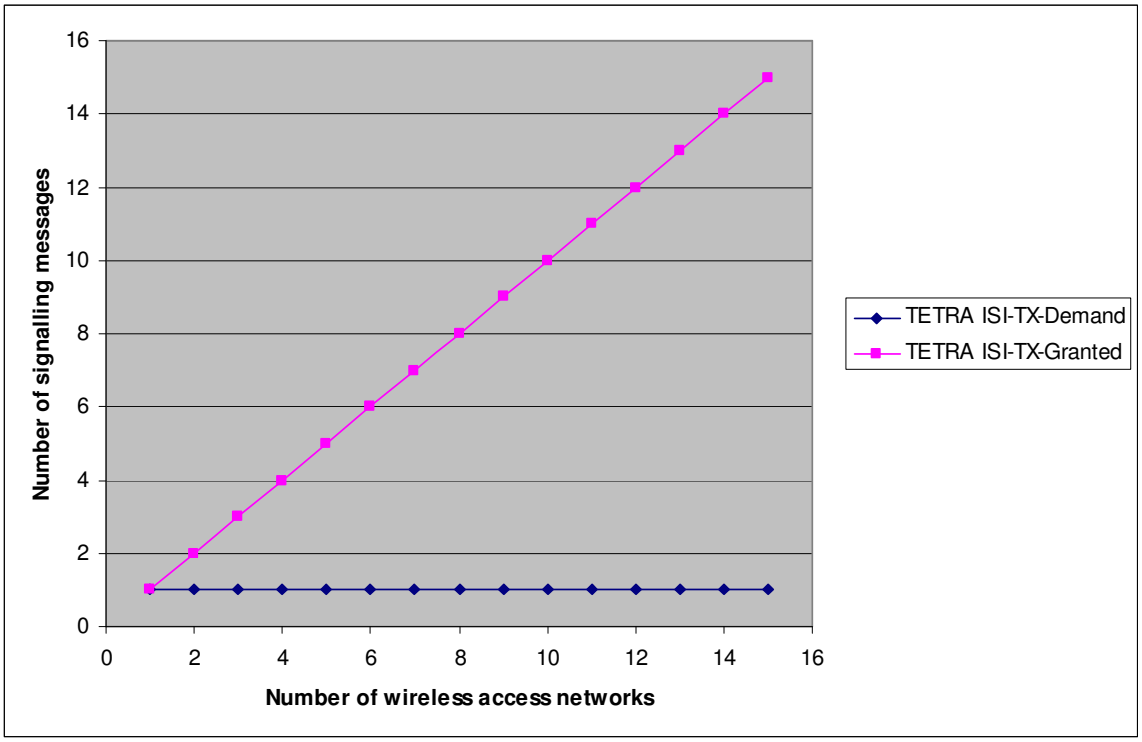

Figure 68: Signaling load vs. wireless access networks for PTT *ODINI way* when using permanently allocated resources policy

5.3.3 Signaling load for PTT Normal way when using temporary allocated resources policy

The message sequence chart associated with this PTT scenario is given and described in Section 4.3.3.3. This message sequence chart is copied in Figure 69.

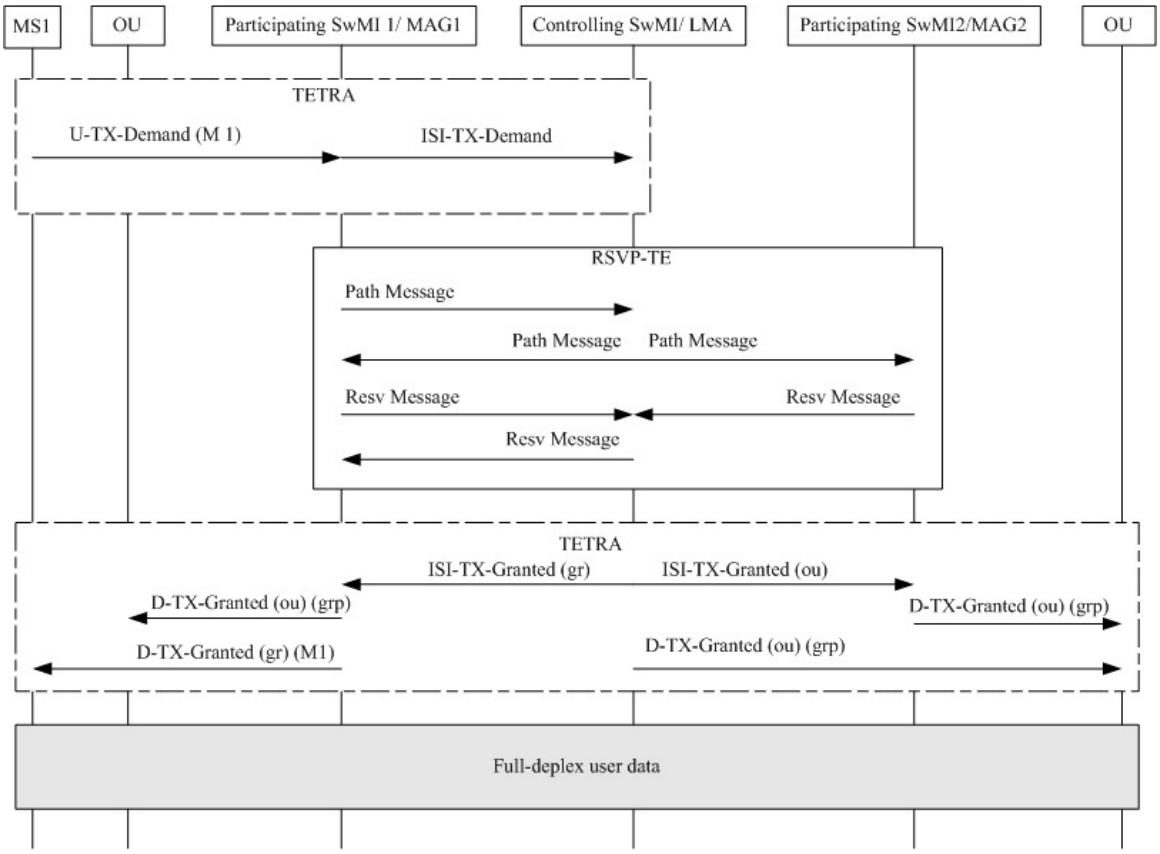

Figure 69: PTT Normal way when using temporary allocated resources policy

By studying this message sequence chart we derived that the number of RSVP_RESV messages and RSVP_Path messages are directly proportional to N+1, where N represents the number of wireless access networks.
Regarding the TETRA _ISI messages identical equations as the ones derived for the previous two PTT procedures apply.
Therefore we derive the following equations for calculating the signaling load for this PTT scenario:

Number of RSVP_Path message=1+N (Eq. 5.19)
Number of RSVP_Resv message=1+N (Eq. 5.20)
Number of TETRA ISI-TX-Demand=1 (Eq. 5.21)
Number of TETRA ISI-TX-Granted=1*N (Eq. 5.22)

Then graphs associated with the above equations can be seen in Figure 70.

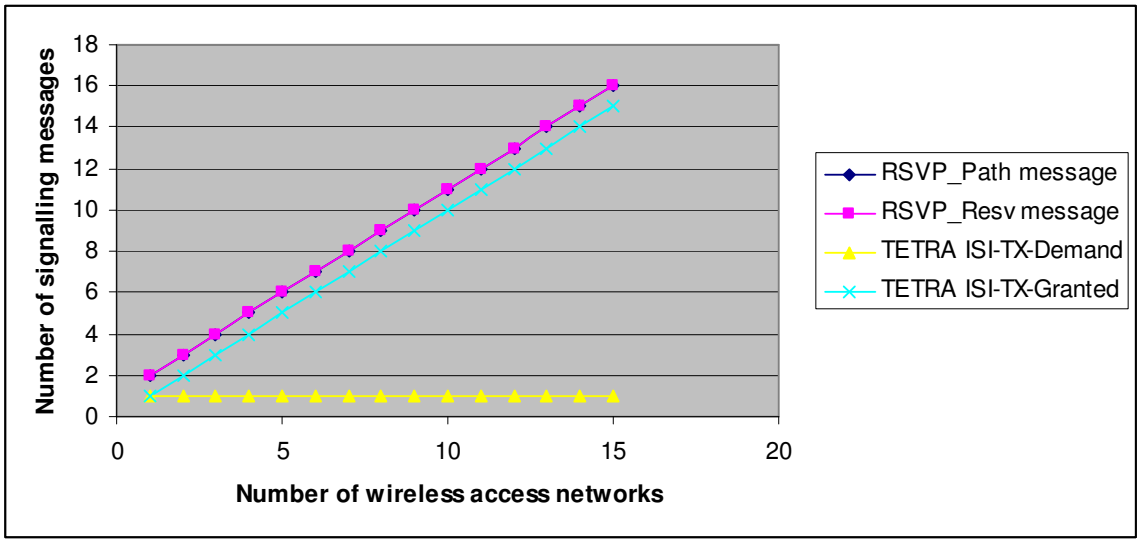

Figure 70: Signaling load vs. wireless access networks for PTT *normal way* when using temporary allocated resources policy

From Figure 70 it can be derived that the numbers of RSVP_Path, RSVP_Resv and TETRA ISI-TX-Granted messages increase linearly when the number of wireless access networks increases. However, the number of TETRA ISI-TX-Demand messages does not depend on the number of wireless access networks and remains equal to 1.

5.3.4 Signaling load for PTT ODINI way when using temporary allocated resources policy

The message sequence chart associated with this PTT procedure is taken from Section 4.3.4 and is shown in Figure 71.

By analyzing the message sequence chart given in Figure 71 we derive identical signaling load equations as the ones derived in Section 5.3.3, see below:

Number of RSVP_Path message=1+N (Eq. 5.23)
Number of RSVP_Resv message=1+N (Eq. 5.24)
Number of TETRA ISI-TX-Demand=1 (Eq. 5.25)
Number of TETRA ISI-TX-Granted=1*N (Eq. 5.26)

Using the above equations we derived the graphs shown in Figure 72.

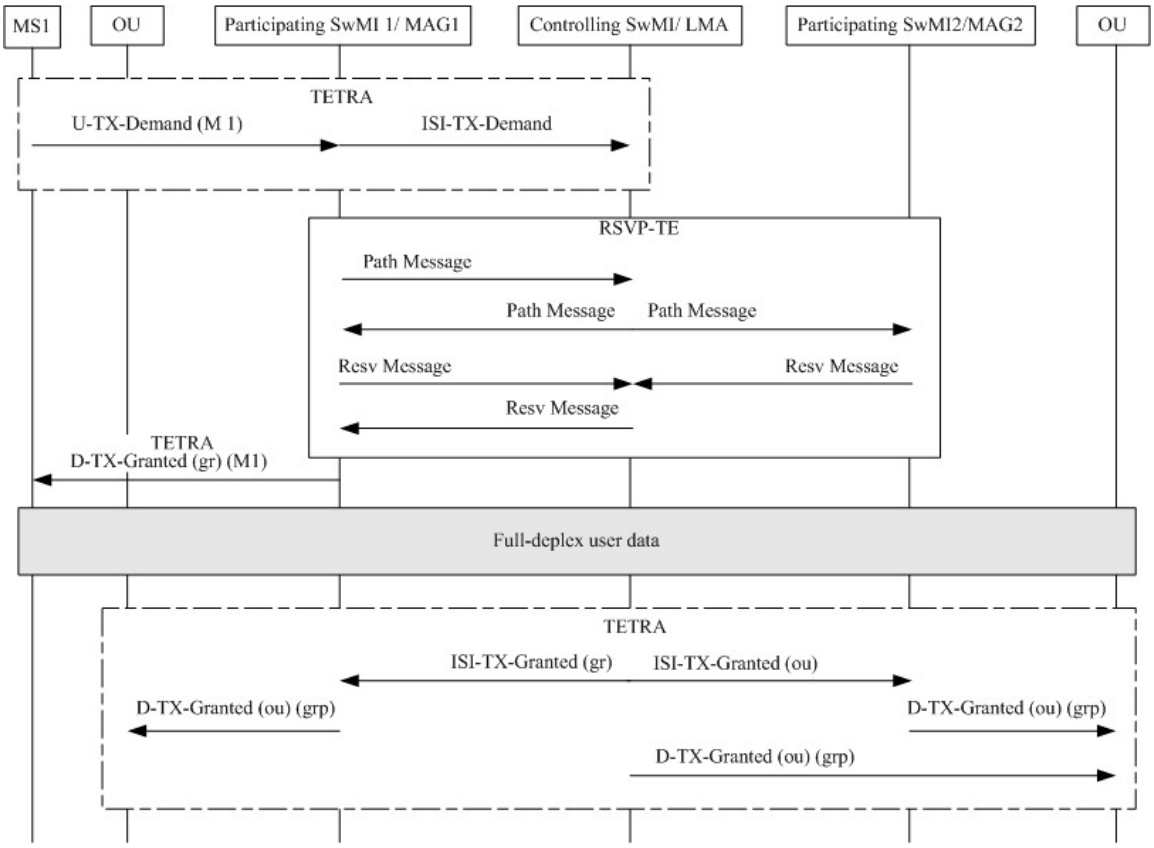

Figure 71: PTT *ODINI way* when using temporary allocated resources policy

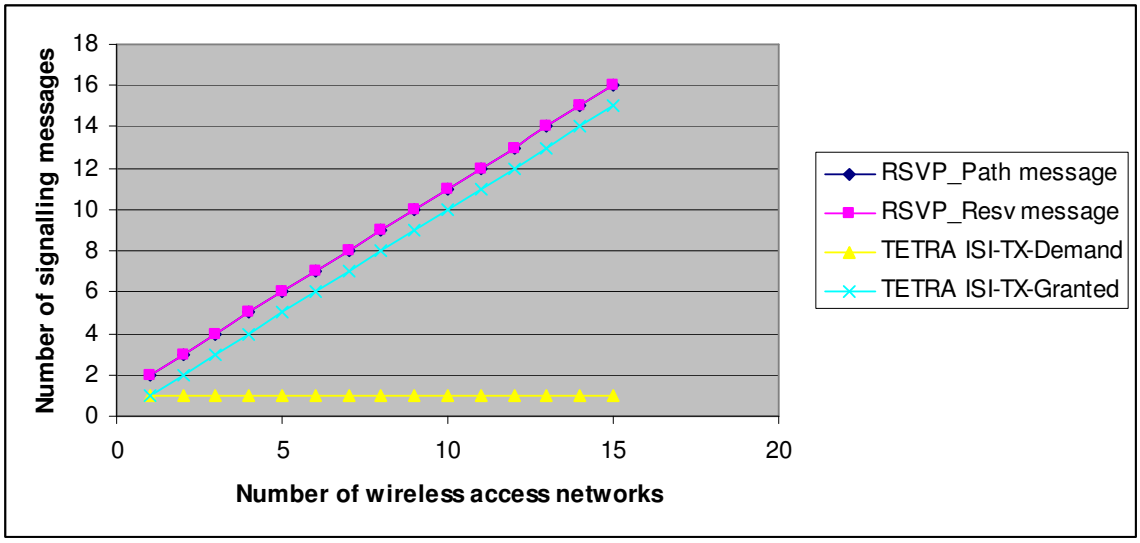

Figure 72: Signaling load vs. wireless access networks for PTT *ODINI way* when using temporary allocated resources policy

5.4 Signaling Load for Call Handover

In this section, we present the scalability analysis of the different handover scenarios. For the call handover, we have only considered the following scenarios: 1. Inter-system Handover for multicast data when using permanently allocated resource policy and when the moving MNs are receivers and 2. Inter-system handover for multicast when using permanently allocated resource policy and when the moving MNs are a transmitters.

5.4.1 Signaling load for handover for multicast when using permanently allocated resources policy and when all the moving users are receivers

The Figure shows the message sequence chart for the inter-system handover for multicast when using permanently allocated resource policy and when MN2 is a receiver, see also Section 4.3.5.1.

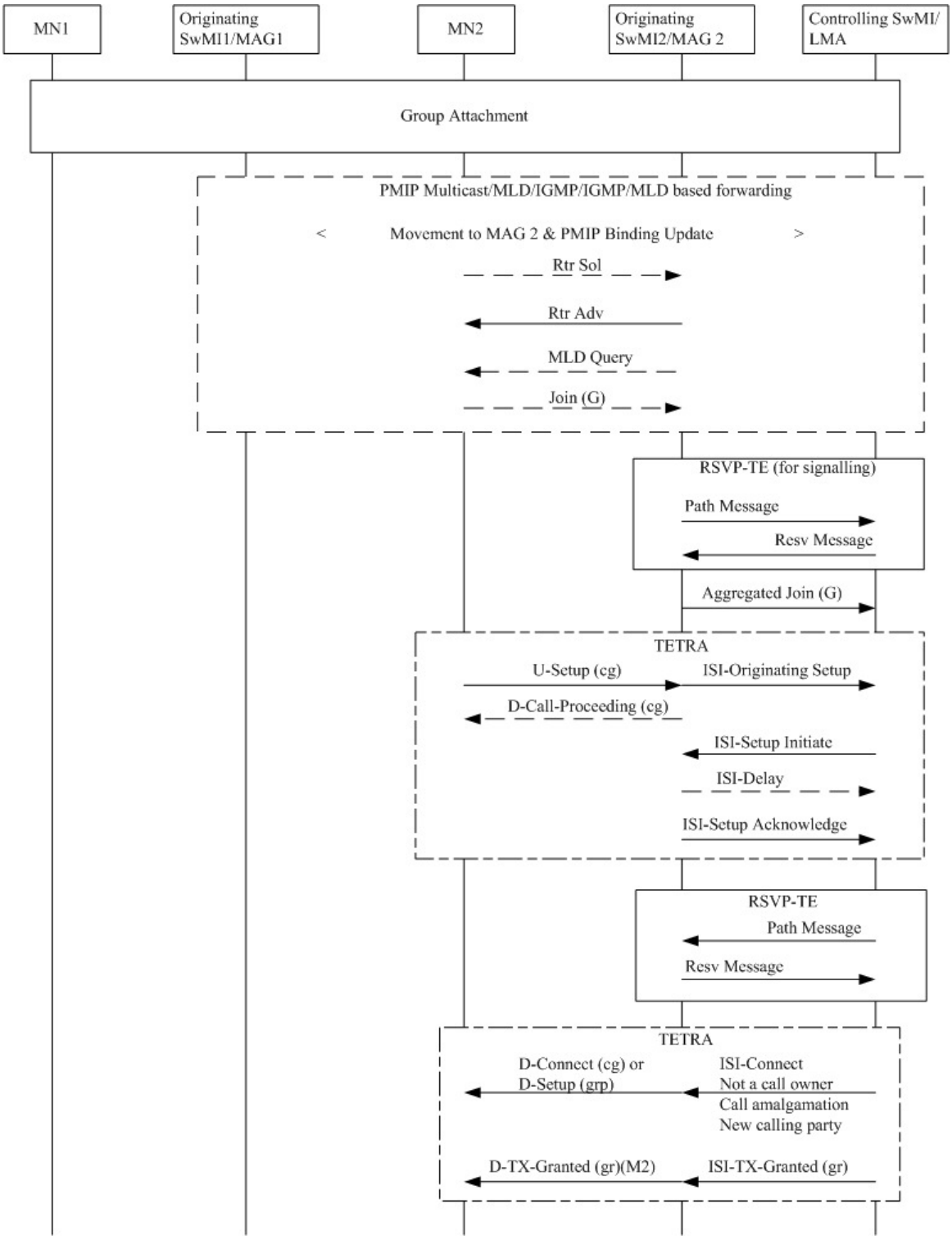

Figure 73: Inter-system handover for multicast when using the permanently allocated resource policy and when moving MN (MN2) is receiver

By analyzing the message sequence chart given in Figure 73 we derived the following signaling load equations, where K represents the number of moving receiving MNs:

Number of RSVP_Path message=2*K (Eq. 5.27)
Number of RSVP_Resv message=2*K (Eq. 5.28)
Number of MLD Aggregated Join=1*K (Eq. 5.29)
Number of TETRA ISI-Originating Setup=1*K (Eq. 5.30)
Number of TETRA ISI-Setup Initiate=1*K (Eq. 5.31)
Number of TETRA ISI-Delay=1*K (Eq. 5.32)
Number of TETRA ISI-Setup Acknowledge=1*K (Eq. 5.33)
Number of TETRA ISI-Connect=1*K (Eq. 5.34)
Number of TETRA ISI-Granted=1*K (Eq. 5.35)

Based on the above equations we derived the signaling load graphs, see Figure 74 associated with this PTT scenario.

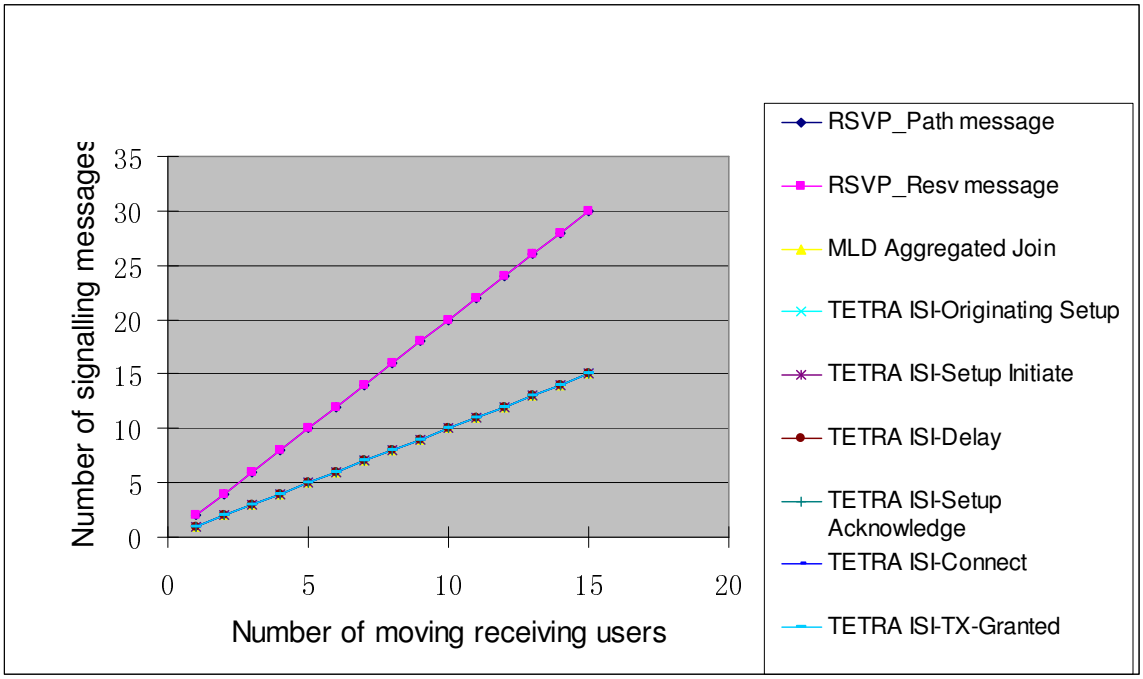

Figure 74: Signaling load for inter-system handover for multicast data when using the permanently allocated resource policy and when moving MNs are receivers

As can be seen in Figure 74, when K increases, the numbers of all the different types of signaling messages increase linearly.

5.4.2 Signaling load for handover for multicast when using permanently allocated resources policy and when all the moving users are transmitters

The message sequence chart associated with this scenario is described in section 4.3.5.2 and it is also depicted in Figure 75.

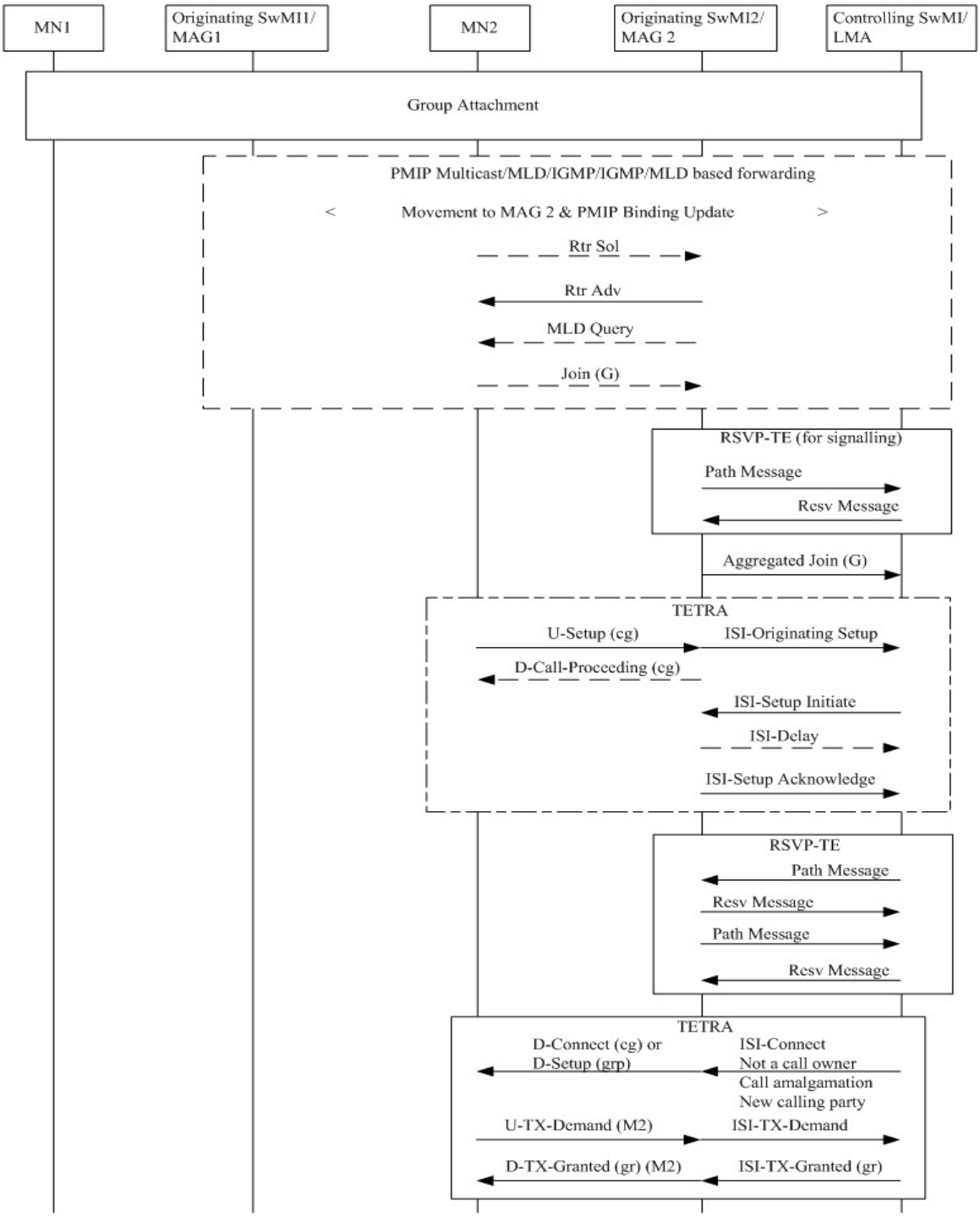

Figure 75: Inter-system handover for multicast data when using the permanently allocated resource policy and when one moving MN (MN2) is a transmitter

Based on the message sequence chart given in Figure 75 we derive the equations associated with this scenario, see below, where Z represents the number of moving transmitting users:

Number of RSVP_Path message= (1+2)*Z (Eq. 5.36)
Number of RSVP_Resv message= (1+2)*Z (Eq. 5.37)
Number of MLD Aggregated Join=1*Z (Eq. 5.38)
Number of TETRA ISI-Originating Setup=1*Z (Eq. 5.39)
Number of TETRA ISI-Setup Initiate=1*Z (Eq. 5.40)
Number of TETRA ISI-Delay=1*Z (Eq. 5.41)
Number of TETRA ISI-Setup Acknowledge=1*Z (Eq. 5.42)
Number of TETRA ISI-Connect=1*Z (Eq. 5.43)
Number of TETRA ISI-Granted=1*Z (Eq. 5.44)
Number of TETRA ISI-Demand=1*Z (Eq. 5.45)

Using the above listed equations we derive the graphs that are depicted in Figure 76.

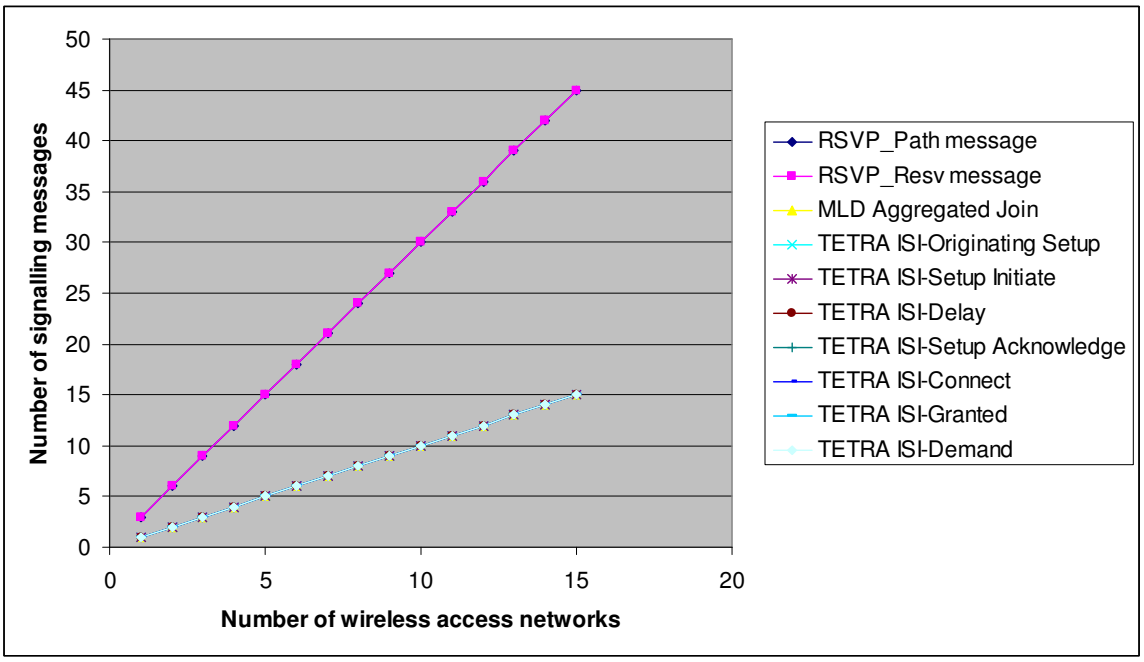

Figure 76: Signaling load for inter-system handover for multicast data when using the permanently allocated resource policy and when moving MNs are transmitters

As can be seen in Figure 76, when Z increases, the numbers of all the different types of signaling messages increase linearly.

5.5 Signaling Load for Call Release

Several call release scenarios have been discussed in Section 4.3.7. In this section, we will only use the scenario entitled as “call disconnection, as a result of calling party disconnecting“, see Section 4.3.7.2, to calculate the signaling load.

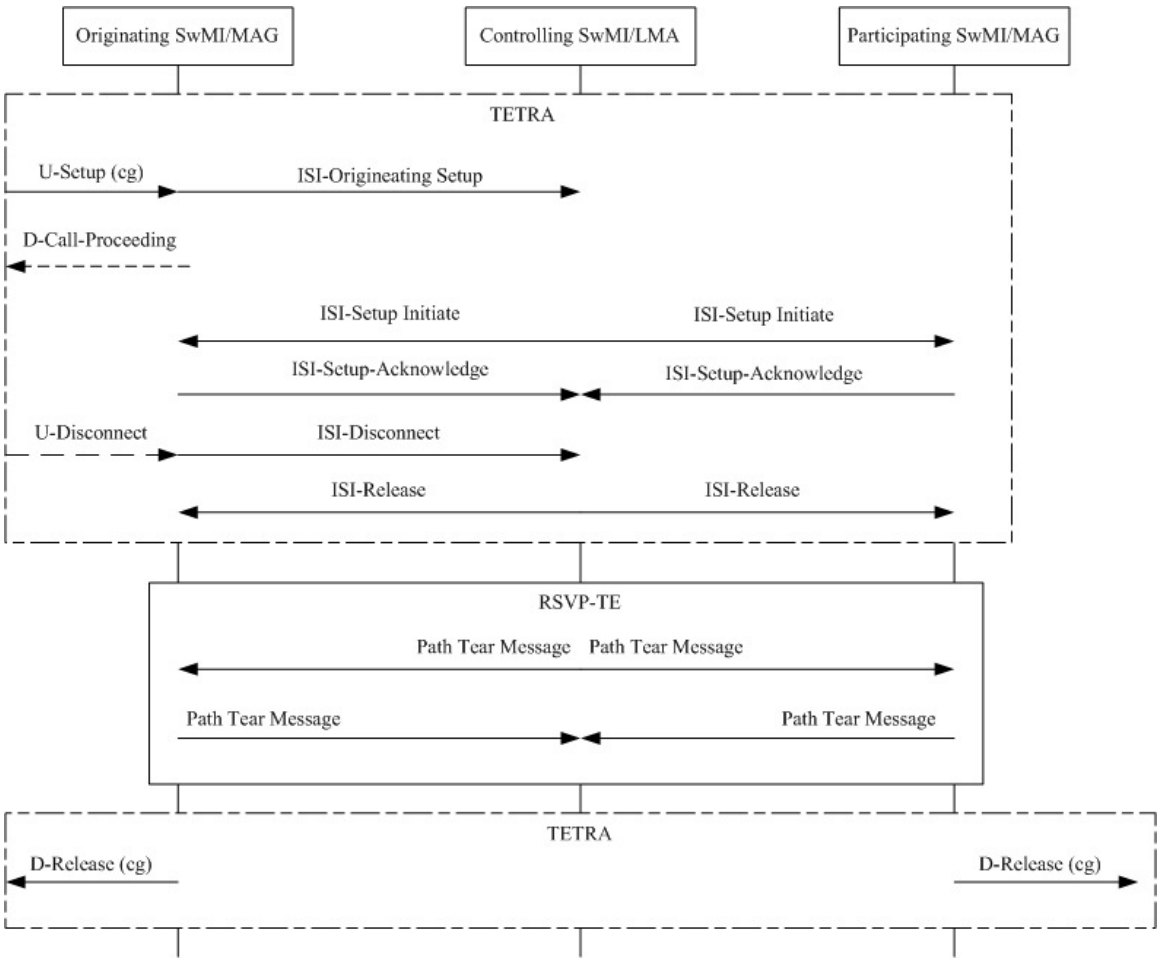

Figure 77: Call disconnection, as a result of calling party disconnecting

The message sequence chart for this call release scenario is shown in Figure 77. Analyzing the message sequence chart given in Figure 77 we derived the following equations, where N is the number of wireless access networks that are supporting group members that are being active in the group call:

Number of TETRA ISI-Originating Setup=1 (Eq. 5.46)
Number of TETRA ISI-Setup Initiate=1*N (Eq. 5.47)
Number of TETRA ISI-Setup Acknowledge=1*N (Eq. 5.48)
Number of TETRA ISI-Disconnect=1*N (Eq. 5.49)
Number of TETRA ISI-Release=1*N (Eq. 5.50)
Number of RSVP_Path_Tear=2*N (Eq. 5.51)

Based on the above equations the signaling load associated with this scenario is derived and depicted in Figure 78.

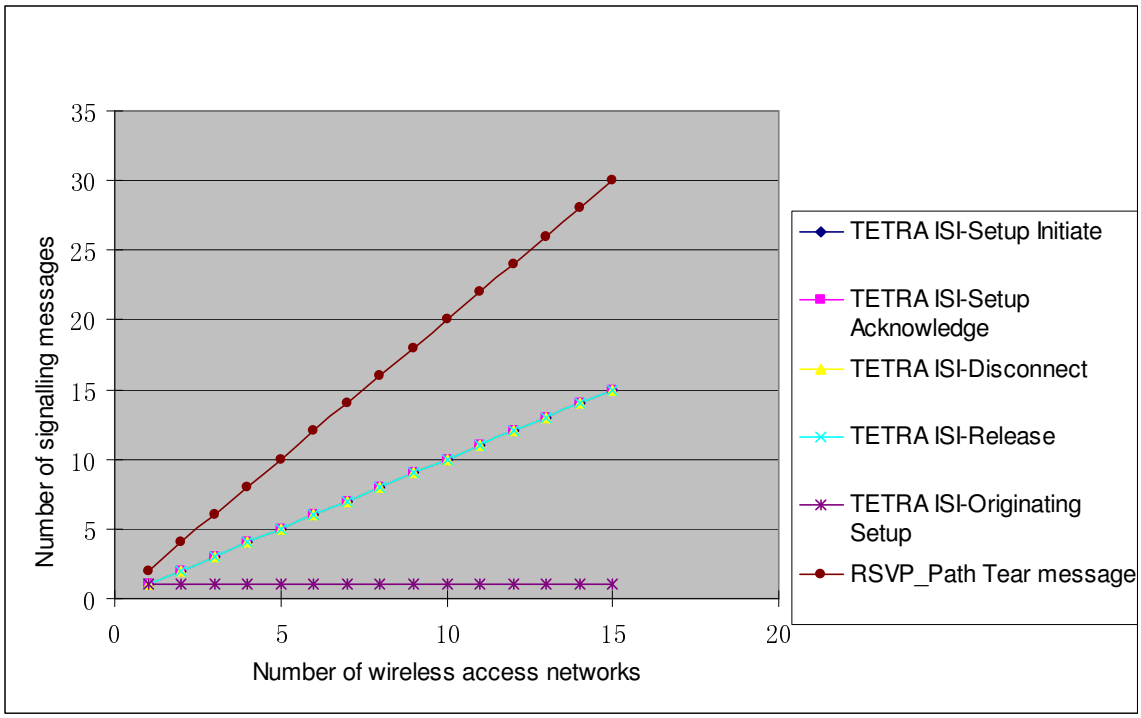

Figure 78: Signaling load vs wireless access networks for call disconnection, as a result of a calling party disconnecting

Since we only have one calling party, the number of TETRA ISI-Originating Setup messages is always one, which does not depend on N. Other TETRA ISI messages increase linearly with the increase of N. The number of RSVP_Path_Tear messages also increases linearly, but with a different slope than the one associated with the TETRA messages.

5.6 Signaling Load for Group Leave

Two types of Group Leave scenarios are described in Section 4.3.6. In this section only the Group Leave scenario is described that is associated with the situation that all the group members are leaving the group. The message sequence chart that shows the situation where all members associated with one wireless access network (i.e., MAG) are leaving an ongoing group is described in Section 4.3.6 and is depicted in Figure 79.

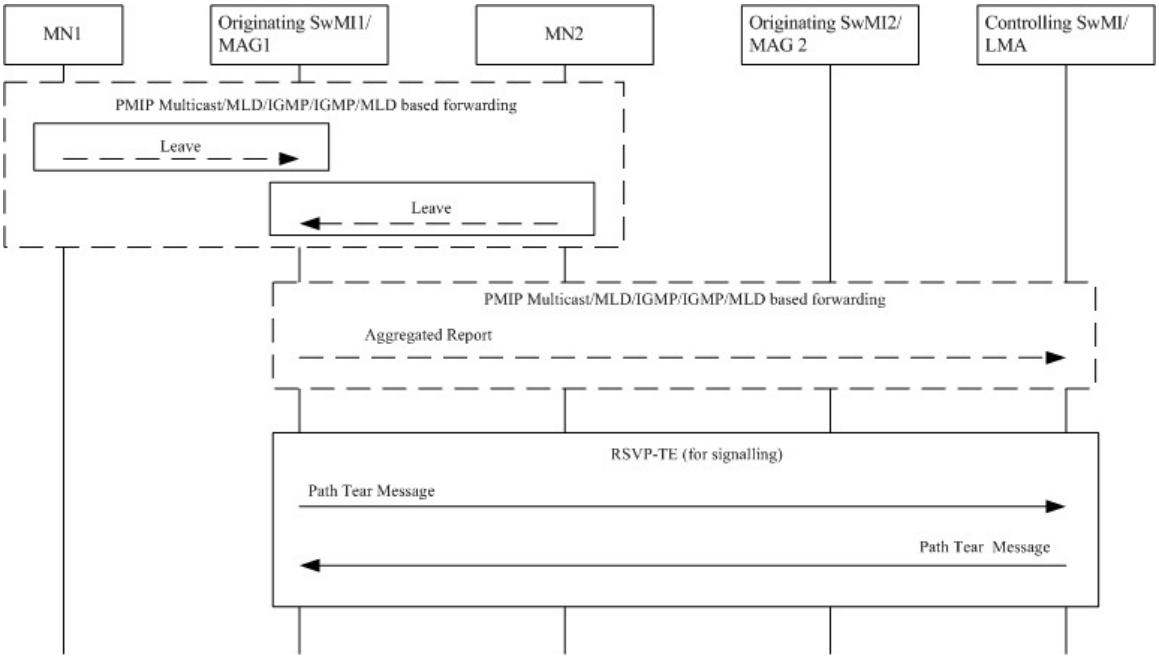

Figure 79: All group members attached to SwMI1/MAG1 leave the group

Based on the message sequence chart given in Figure 79, we derive the signaling load equations associated with this scenario:

The following signaling load equations are derived considering that the number (N) of wireless access networks (MAGs) that are supporting group members which are leaving is increased:

Number of MLD aggregated report=1*N (Eq. 5.52)
Number of RSVP_Path_Tear message=2*N (Eq. 5.53)

Based on these two equations, the signaling load for group leave is derived and is given in Figure 80.

Both MLD aggregated report and RSVP_Path_Tear message increase linearly when the number (N) of wireless access networks (MAGs) that are supporting group members which are leaving is increased.

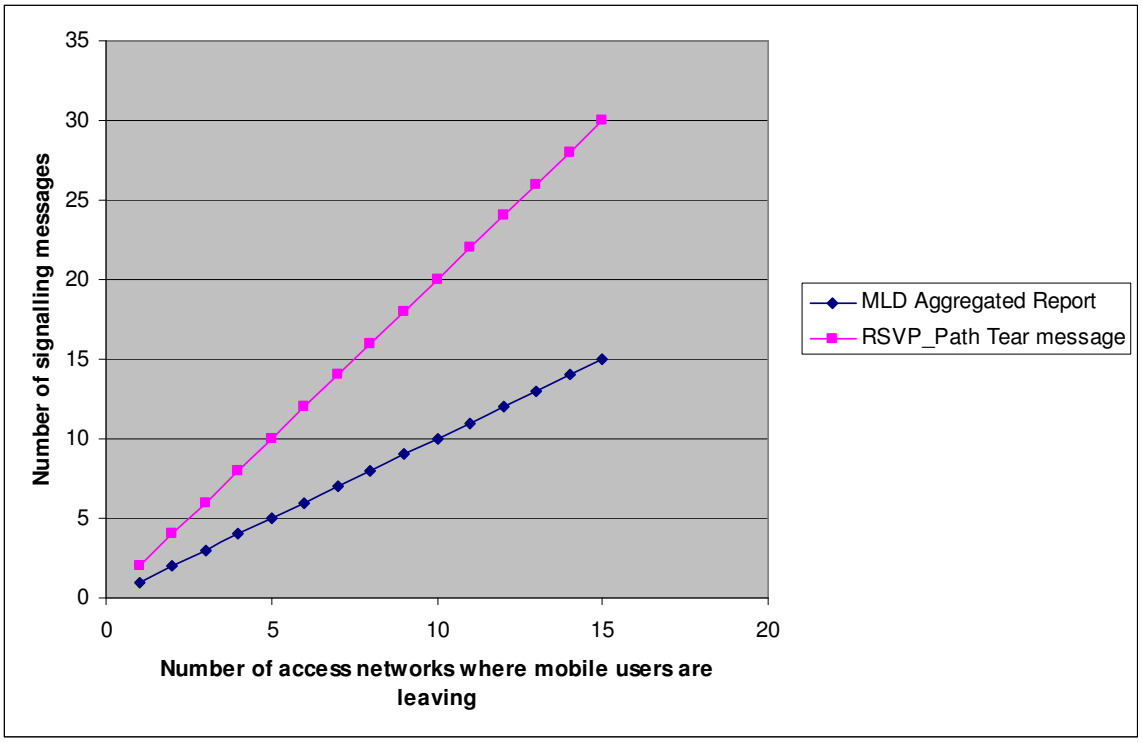

Figure 80: Signaling load vs wireless access networks when all users attached to wireless access networks are leaving the group

Chapter 6: Conclusion and future work

This chapter concludes this M.Sc. thesis and points out recommendations for further research. In Section 6.1, the conclusions derived by this M.Sc. thesis are provided. The answers to research questions are presented in section 6.2. In Section 6.3, the main contributions of this thesis project are highlighted. Finally, the recommendations for future work are discussed in Section 6.4.

6.1 Conclusions

The first step in this M.Sc. assignment was to identify the current mission-critical services that are provided by TETRA. Afterwards, the network scenarios that could support these mission critical services were identified. Based on the identified mission-critical services and the selected three network scenarios, we derived a list of core network architecture requirements for the interconnection of heterogeneous wireless access networks, e.g., TETRA, WiMAX, UMTS, and LTE. By doing a literature study a list of existing standardized solutions that can fulfill these architecture requirements was found. The core network architecture has been designed based on these existing standardized solutions, which are: TETRA, Proxy Mobile IP, MPLS, RSVP-TE and RSVP-TE with multicast. In short, in order to provide the TETRA based mission-critical communication services, it is possible to design a core network architecture that can interconnect heterogeneous wireless access networks.

Based on the TETRA ISI message sequence charts, we defined enhanced ISI message sequence charts for group call's main steps: group establishment, call setup, push to talk & call maintenance, call handover, group leave and call release. These enhanced ISI message sequence charts are used to specify how the core network architecture can support the interworking and interoperation of the available TETRA, MPLS, Proxy Mobile IP and RSVP-TE solutions and/or protocols such that the interconnection of various wireless communication systems is accomplished.

After the core network architecture has been specified, we evaluated it by using scalability as performance metric. In particular we derived a number of equations that we used to calculate the number of signaling messages generated by various types of signaling procedures when either the number of wireless access networks is increased or when the number of users that are roaming is increased.
Specifically, for the main steps such as group establishment, call setup, push to talk, call release and group leave, the signaling load is derived with respect to the number of wireless access networks. For call handover, the signaling load is derived with respect to the number of moving transmitting or receiving users.

TETRA ISI messages are applicable to the call setup, handover and call release. The evaluation results show that for these three main signaling steps, the number of (almost all) the TETRA ISI messages increases linearly. The numbers of TETRA ISI-Originating

Setup and TETRA ISI-TX-Demand messages remain constant even if the number of active wireless access networks increases.
RSVP_Resv and RSVP_Path message are applicable to group establishment, call setup, call handover and PTT (Push-To-Talk) when using the temporary allocated resources policy. According to the evaluation results, for group establishment and PTT, the numbers of RSVP_Resv and RSVP_Path messages increase linearly. For the call setup scenario, the situation is different than other steps. When the RSVP-TE procedures are setting up point to multipoint LSPs the number of RSVP_Resv and RSVP_Path messages increases linearly. However, when the RSVP-TE procedures are setting up multipoint to multipoint LSPs then the number of RSVP_Resv and RSVP_Path messages grows exponentially. For handover when all the moving users are either receivers or transmitters, the numbers of RSVP_Resv and RSVP_Path messages grow linearly.

The behavior of *MLD aggregated join* and *MLD aggregated report* procedures are only applicable for the group attachment. The numbers of *MLD aggregated join* and *MLD aggregated report* messages increase linearly. The RSVP_Path_Tear messages are used the group leave and call release procedures. The number of RSVP_Path_Tear messages grows linearly with the increase of the wireless access networks.

6.2 Answers to Research Questions

In the chapter one, we defined five research questions. These research questions are answered as follows:
(1) What are the application scenarios for mission-critical group communications?

According to [ODINI], there are three network scenarios that can be used to support mission-critical services for group communications. These three network scenarios are Tactical Patch, Expanding Coverage and Migration to other network. Tactical patch has two categories: one is cross-border cooperation and another is inter-agency cooperation.

(2) What are the requirements imposed by these application scenarios on the core network architecture used to interconnect heterogeneous wireless communication systems?

From the description of mission critical services and three network scenarios, we derived a list of requirements: strict QoS support (with many priority levels (8 levels at least) and preemption support), security, reliability, mode of communication, scalability and robustness.

(3) Are there any existing standardized solutions that can fulfill these requirements?

After performing a literature study, a list of existing standardized solutions that can fulfill these architecture requirements are found: RSVP, RSVP-TE, MPLS, GMPLS, MPLS Multicast Encapsulations, Differentiated services (Diffserv), Integrated services (Intserv), MPLS support for Differentiated Services, IGMPv3, MLDv2, IGMP/MLD-Based

Multicast Forwarding, Distance Vector Multicast Routing Protocol (DVMRP), Multicast Open Shortest Path First (MOSPF), Protocol Independent Multicast-Sparse Mode (PIM-SM), Protocol Independent Multicast-Dense Mode (PIM-DM), Mobile IP (MIP), Proxy Mobile IP (PMIP), Network Mobility, Multicast Listeners in PMIPv6, Security Framework for MPLS and GMPLS Networks and IPSec.

(4) What are the core network architectural building blocks used for the interconnection of heterogeneous wireless communication systems applied for mission-critical group communications?

To answer this research question, we investigated the existing standardized solutions and we could derive and propose a core network architecture that is based on MPLS. The core network architectural building blocks are the gateway (i.e., LER, LMA, MAG, and SwMI) and interior core router (i.e., LSR). They both support several functionalities that are required to support the interconnection of heterogeneous wireless communication systems applied for mission-critical group communications.

(5) How could this core network architecture be evaluated?

This core network architecture can be evaluated using several performance measures, such as latency, throughput, signaling load scalability, etc. Due to time constraints, only the signaling load scalability is considered in this M.Sc. thesis. We choose a number of ISI signaling scenarios that are associated with the main group call steps. Then by deriving equations to calculate the signaling load, several charts are made to show the signaling message load of the different group call steps, when increasing either the number of wireless access networks, or the number of moving users.

6.3 Contribution

The contribution of this M.Sc. project is summarized as follows:

- Specification and design of a core network architecture used to enhance the existing protocols or solutions that are standardized by IETF and TETRA.
- Protocols required in core network architecture are identified.
- Certain interworking features that are needed in order to support the interoperation between protocols used within the TETRA network and the ones used core network are defined using signaling message sequence charts.
- The core network architecture is evaluated using scalability. Signaling load charts are generated to show the signaling load scalability of various signaling messages in all the group call steps, when either the number of wireless access networks or the number of moving users is increased.

6.4 Future work

In this M.Sc. project, due to time constraints we only investigated the scalability of the core network architecture. We calculated the signaling load scalability of the different types of signaling procedures associated with the group call service. Since for mission-critical group communication, other services are also important, we could calculate the signaling load that is transported in the core network architecture for other basic services as well as supplementary services.

Furthermore, it is recommended to evaluate the core network architecture using other performance measures, such as latency, throughput, jitter, robustness and security etc. Possibly, the evaluation of the core network architecture with respect to the mentioned performance measures can be done by using simulation experiments. The extensive simulation experiments could be performed to test the functionalities of the network entities and investigate the architecture's performance behavior when different services are supported.

Bibliography

[DuGi99] John Dunlop, Demessie Girma, James Irvine, “Digital Mobile Communications and the TETRA System”, WILEY 1999.

[Deer91] Deering, S., "Multicast Routing in a Datagram Internetwork", Ph.D. Thesis, Stanford University, December 1991.

[ETSI TETRA] Official website of ETSI TETRA (visited in November 2010) http://www.etsi.org/website/Technologies/TETRA.aspx

[ETS-300392-3-1] “Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-system Interface (ISI); sub-part 1: General design”, ETSI TETRA specification, ETS 300392-3-1, January 1999.

[ETSI-EN-300392-3-3] “Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-system Interface (ISI); Sub-part 3: Additional Network Feature Group Call (ANF-ISIGC)”, ETSI TETRA specification, ETSI EN 300392-3-3, January 2004.

[ETSI-TS-100392-3-2] “Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-system Interface (ISI); Sub-part 3: Additional Network Feature Individual Call (ANF-ISIIC)”, ETSI TETRA specification, ETSI TS 100392-3-2, October 2000.

[ETSI-TR-300-1] “Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Designers' guide; Part 1: Overview, technical description and radio aspects”, ETSI TETRA specification, ETSI TR 300-1, May 1997.

[ETSI-EN-300392-3-4] “Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-system Interface (ISI); Sub-part 3: Additional Network Feature Short Data

Service (ANF-ISISDS)", ETSI TETRA specification, ETSI EN 300392-3-4, January 2004.

[ETSI-TR-086-2] "Terrestrial Trunked Radio (TETRA) system, Technical requirements specification, Part 2: Packet Data Optimized (PDO) systems", ETSI TETRA specification, ETSI TR 086-2, January 1994.

[ETSI-TR-086-3] "Terrestrial Trunked Radio (TETRA) systems; Technical requirements specification, Part 3: Security aspects", ETSI TETRA specification, ETSI TR 086-3, January 1994.

[ETSI-EN-300392-1] "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design", ETSI TETRA specification, ETSI EN 300392-1, January 2009.

[ETSI-EN-300392-10-16] "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 16: Pre-emptive Priority Call (PPC)", ETSI TETRA specification, ETSI EN 300392-10-16, August 2006.

[ETS-300392-10-24] "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 24: Call Retention", ETSI TETRA specification, ETS 300392-10-24, April 2000.

[ETSI-EN-300392-10-10] "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 10: Priority Call", ETSI TETRA specification, ETSI EN 300392-10-10, May 2002.

[ETSI-EN-300392-10-22] "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 22: Dynamic Group Number Assignment (DGNA)", ETSI TETRA specification, ETSI EN 300392-10-22, January 2002.

[ETSI-EN-300392-10-21] "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 21: Ambience Listening (AL)", ETSI TETRA specification, ETSI EN 300392-10-21, September 2003.

[ETSI-EN-300392-10-6] "Terrestrial Trunked Radio (TETRA); Voice plus Data

(V+D); Part 10: Supplementary services stage 1; Sub-part 6: Call Authorized by Dispatcher (CAD)", ETSI TETRA specification, ETSI EN 300392-10-6, August 2006.

[ETSI-EN-300392-10-8] "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 8: Area Selection (AS)", ETSI TETRA specification, ETSI EN 300392-10-8, February 2004.

[ETSI-EN-300392-10-14] "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 14: Late Entry", ETSI TETRA specification, ETSI EN 300392-10-14, September 2002.

[ETSI-ETS-300392-3-5] "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 5: Additional Network Feature for Mobility Management (ANF-ISIMM)", ETSI TETRA specification, ETSI ETS 300392-3-5, January 2000.

[ETSI-ETS-300392-2] "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)", ETSI TETRA specification, ETSI-ETS-300392-2, September 2007.

[IEEE Ethernet] Official website of IEEE 802.3 Ethernet Working Group (visited in November 2010) http://www.ieee802.org/3/

[MeBo76] R,Metcalfe, D.Boggs, "Ethernet: Distributed Packet Switching for Local Computer Networks", in Communications of the ACM, Vol.19, no.5, pp.395-405,1976.

[multimob] Official web site of IETF MULTIMOB Working Group (visited in November 2010) https://datatracker.ietf.org/wg/multimob/charter/

[ODINI] ROHILL Whitepaper "On-Demand-Intelligent Network Interface (ODINI)", ROHILL, October 2009, to be found (visited in November 2010) http://www.odini.org/odini/images/rohill/whitepaper%20o

dini%20issue%201.1.pdf

[ODINI_slides] B. Bouwers, “TETRA moving forward in China Networking Innovations”, ROHILL slides, 2009, to be found (visited in November 2010) via: http://www.tetramou.com/uploadedFiles/Files/Presentations/China2009bertbouwers.pdf

[ODINI_patent] E. Bouwers, "Fast inter system push to talk operation", ROHILL Technologies, European Patent Application, Nr. EP 2 160 050 A1, 3 March 2010.

[RFC768] J. Postel, “User Datagram Protocol”, IETF RFC 768, August 1980.

[RFC791] J. Postel, “Internet Protocol”, IETF RFC 791, September 1981.

[RFC793] J. Postel, “Transmission Control Protocol”, IETF RFC 793, September 1981.

[RFC1075] D. Waitzman, C. Partridge, S. Deering, “Distance Vector Multicast Routing Protocol”, IETF RFC 1075, November 1988.

[RFC1058] C. Hedrick, “Routing Information Protocol”, IETF RFC 1058, June 1988.

[RFC1112] S. Deering, “Host Extensions for IP Multicasting”, IETF RFC 1112, August 1989.

[RFC1585] J. Moy, “MOSPF: Analysis and Experience”, IETF RFC 1585, March 1994.

[RFC1583] J. Moy,” OSPF Version 2”, ETF RFC 1583, March 1994.

[RFC1633] R. Braden, D. Clark, S. Shenker, “Integrated Services in the Internet Architecture: an Overview”, IETF RFC 1633, June 1994.

[RFC2205] R. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin, “Resource ReSerVation Protocol --Version 1 Functional Specification”, IETF RFC 2205, September 1997.

[RFC2236] W. Fenner, “Internet Group Management Protocol, Version 2”, IETF RFC 2236, November 1997.

[RFC2401] S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol”, IETF RFC 2401, November 1998.

[RFC2460] S. Deering, R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification”, IETF RFC 2460, December 1998.

[RFC2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, “An Architecture for Differentiated Services”, IETF RFC 2475, December 1998.

[RFC2710] S. Deering, W. Fenner, B. Haberman,”Multicast Listener Discovery (MLD) for IPv6”, IETF RFC 2710, October 1999.

[RFC3031] E. Rosen, A. Viswanathan, R. Callon, “Multiprotocol Label Switching Architecture”, IETF RFC 3031, January 2001.

[RFC3032] E. Rosen, D. Tappan, G. Fedorkow, Y. Rekhter, D. Farinacci, T. Li, A. Conta,” MPLS Label Stack Encoding”, IETF RFC 3032,January 2001

[RFC3209] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, G. Swallow, “RSVP-TE: Extensions to RSVP for LSP Tunnels”, IETF RFC 3209, December 2001.

[RFC3270] F. Le Faucheur, L. Wu, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, J. Heinanen, “Multi-Protocol Label Switching (MPLS) Support of Differentiated Services”, IETF RFC 3270, May 2002.

[RFC3376] B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan,” Internet Group Management Protocol, Version 3”, IETF RFC 3376,October 2002.

[RFC3344] C. Perkins,” IP Mobility Support for IPv4”, IETF RFC3344, August 2002.

[RFC3353] D. Ooms, B. Sales, W. Livens, A. Acharya, F. Griffoul, F. Ansari," Overview of IP Multicast in a Multi-Protocol Label Switching (MPLS) Environment", IETF RFC 3353, August 2002.

[RFC3473] L. Berger, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", IETF RFC 3473, January 2003.

[RFC3775] D. Johnson, C. Perkins, J. Arkko," Mobility Support in IPv6", IETF RFC 3775, June 2004.

[RFC3810] R. Vida, L. Costa," Multicast Listener Discovery Version 2 (MLDv2) for IPv6", IETF RFC 3810, June 2004.

[RFC3945] E. Mannie, "Generalized Multi-Protocol Label Switching (GMPLS) Architecture", IETF RFC 3945, October 2004.

[RFC3973] A. Adams, J. Nicholas, W. Siadak, "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)", IETF RFC 3973, January 2005.

[RFC3963] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert," Network Mobility (NEMO) Basic Support Protocol", IETF RFC 3963, January 2005.

[RFC4080] R. Hancock, G. Karagiannis, J. Loughney, S. Van den Bosch, "Next Steps in Signaling (NSIS): Framework", IETF RFC 4080, June 2005.

[RFC4301] S. Kent, K. Seo, "Security Architecture for the Internet Protocol", IETF RFC 4301, December 2005.

[RFC4601] B. Fenner, M. Handley, H. Holbrook, I. Kouvelas," Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", IETF RFC 4601, August 2006.

[RFC4605] B. Fenner, H. He, B. Haberman, H. Sandick, "Internet

Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding", IETF RFC 4605, August 2006.

[RFC4875] R. Aggarwal, D. Papadimitriou, S. Yasukawa, "Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)", IETF RFC 4875, May 2007.

[RFC5177] K. Leung, G. Dommety, V. Narayanan, A. Petrescu," Network Mobility (NEMO) Extensions for Mobile IPv4", IETF RFC 5177, April 2008.

[RFC5186] B. Haberman, J. Martin, "Internet Group Management Protocol Version 3 (IGMPv3) / Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction", IETF RFC 5186, May 2008.

[RFC5213] S. Gundavelli, Ed., K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, "Proxy Mobile IPv6", IETF RFC 5213, August 2008.

[RFC5332] T. Eckert, E. Rosen, R. Aggarwal, Y. Rekhter, "MPLS Multicast Encapsulations", IETF RFC 5332, August 2008.

[RFC5757] T. Schmidt, M. Waehlisch, G. Fairhurst, "Multicast Mobility in Mobile IP Version 6 (MIPv6): Problem Statement and Brief Survey", IETF RFC 5757, February 2010.

[RFC5844] R. Wakikawa, S. Gundavelli," IPv4 Support for Proxy Mobile IPv6", IETF RFC 5844, May 2010.

[RFC5920] L. Fang, "Security Framework for MPLS and GMPLS Networks", IETF RFC 5920, July 2010.

[RFC5971] H. Schulzrinne, R. Hancock, "GIST: General Internet Signalling Transport", IETF RFC5971, October 2010.

[RFC5974] J. Manner, G. Karagiannis, A. McDonald, "NSIS Signaling Layer Protocol (NSLP) for Quality-of-Service Signaling", IETF RFC 5974, October 2010.

[Salk06] A.K. Salkintzis, "Evolving Public Safety Communication Systems by Integrating WLAN and TETRA networks", in IEEE Communications Magazine, Vol. 44, Issue 1, pp. 38 – 46, January 2006.

[ScWa10] T C. Schmidt, M. Waehlisch, S. Krishnan, "Base Deployment for Multicast Listener Support in PMIPv6 Domains", IETF Internet-Draft, draft-ietf-multimob-pmipv6-base-solution-06, Work in progress, October 2010.

[StZh99] I. Stoica, H. Zhang, "Providing guaranteed services without per flow management", Proc. of SIGCOMM: Applications, technologies, architectures, and protocols for computer communication, SIGCOMM'99, 1999.

[SiSh96] C.A.Siller, M.Shafi, editors, "SONET/SDH: A Sourcebook of Synchronous Networking", IEEE Press, 1996.

[TETRA-A] Official website of TETRA Association (visited in November 2010) http://www.tetramou.com/tetramou.aspx?id=44

[TETRAPOL] Official website of TETRAPOL (visited in November 2010): http://www.tetrapol.com/home/tetrapol