3

Coalition Networks for Secure Information Sharing

3

Final Report – Task 1

CoNSIS

Document CoNSIS/Task 1/DU/001

August 30, 2013

Record of Amendments

Amendment Number	Amendment Pages	Date Entered	Signature
1	All	30.10.12	hse
2	All	20.11.12	hse
3	All	25.11.12	hse
4	Many	29.11.12	Mariann
5	Comments	03.12.12	hse
6	Final Version	08.12.12	hse
7	NOR Com-ments and USA input	24.01.13	hse
8	All	30.08.13	hse

0. ABSTRACT

Secure information exchange is a key success factor for military operations. International coalition missions are especially challenging because of heterogeneous communication and C2IS equipment. The multinational project CoNSIS is targeted to fill in technical gaps regarding interoperability which occur in a reference scenario, consisting of a multinational convoy of military and non-governmental vehicles, a maritime group and some deployed headquarters. The convoy forms an ad-hoc radio network and shares a common operational picture with a coalition headquarter mainly via a satellite link. This paper addresses network challenges and technical solutions for this federated scenario. Both the core network interconnecting different national headquarters with an international headquarter as well as the ad-hoc radio network of the convoy are addressed in a single, seamless concept. In June 2012, field tests with the convoy were carried out in order to evaluate the different technical solutions.

The purpose of Task 1 was to provide and maintain a seamless and robust internetwork solution, based on various, heterogeneous tactical radio equipment. It was specified and validated that existing tactical radios can be (easily) included into a common network scenario on an ad-hoc basis.

Task1 has also studied and implemented several mechanisms to support end-to-end differentiated quality of service through the heterogeneous mobile ad hoc coalition network and through the heterogeneous deployed coalition backbone network. These solutions can also be used to aid an admission control and resource management element in the network.

Requirements are formulated that describe necessary actions to get a common network running based on randomly interconnected (national) network segments and how to handle various resource parameters in a permanently changing and disturbed (jammed) environment. All these results can be described as a standardized network profile, which is than a basis for upper layer usage, which express their requirements towards this transparent network interface and which consumes the results being reported from the internetwork layer towards these applications.

When interconnecting radio equipment from various nations, a minimum set of rules shall be followed. Mechanisms being used in one segment shall not be foiled by another mechanism from another segment. To avoid such a situation, a minimum pre-planning is necessary to describe interoperable protocol mechanisms across a number of network segments within a standardized profile.

Table of Contents

Table of Figures

Table of Tables

1. INTRODUCTION

The Coalition Network for Secure Information Sharing (CoNSIS) is a multinational group consisting of members from France, Germany, Norway, and USA, with participants from both research institutions and industry. The objectives of this group are to develop, implement, test, and demonstrate technologies and methods that will facilitate the partners' abilities to share information and services securely in ad-hoc coalitions, and between military and civil communication systems, within the communications constraints of mobile tactical forces.

The group has focused on practical application of information infrastructure technologies in a network-of-networks, consisting of a variety of low capacity and capability network technologies. The work done within the CoNSIS group has been divided into a number of tasks, each focusing on a different aspect of interoperability issues. This report covers the domain of tactical network and communications concepts with mainly limited network capacities. During June 2012 CoNSIS conducted a large-scale experiment in Greding, Germany, in which all the different aspects of technical interoperability were tested; integrating the work of all the task groups of CoNSIS.

The remainder of this report is structured as follows

- Chapter 2 provides an introduction to CoNSIS and the different task groups
- Chapter 3 introduces the network and communication concept in CoNSIS
- Chapter 4 describes the CoNSIS experimentation results in Greding
- Chapter 5 contains the conclusion for task 1 and describes possible further work in phase 2

2. CONSIS

The CONSIS areas of work are broken down into five major tasks as follows:

- Task 1 - Communication Services
- Task 2 - Information and Integration Services (SOA)
- Task 3 - Security
- Task 4 - Management
- Task 5 - Architecture, Test & Demonstration, and Coordination

Task 1 has focused on activities to support a general goal of an overall NII infrastructure based on IP technology. The focus of this task has been on demonstrating solutions that will work within the communications constraints and dynamic topology imposed by highly mobile tactical networks. Communication services within tactical systems have been analyzed towards their ability to support SOA core services (e.g. discovery), real time services (e.g. VoIP and VTCoIP) and streaming services (e.g. TADIL).

Task 2 has demonstrated the applicability of the SOA approach in a multinational military environment, federating the SOAs of each nation. The task has been taking into account the constraints of security and the constraints applicable to highly mobile tactical forces (including limited bandwidth, intermittent communications, high rate of change of network topology, and the need to make decisions quickly).

Task 3 investigated, specified, and demonstrated security mechanisms for use for integration and interoperability of heterogeneous, coalition networks. The likely next expansion of military networks will be into highly mobile platforms on the tactical edge. A second area of interest has been to develop and demonstrate practical, yet secure, black-core, network topologies and architectures for coalition interoperability. A third area of interest has been to investigate the use of Multilevel Security (MLS) including the use of virtual terminal technology for cross-domain solutions that support network communications operating at multiple security levels without separate infrastructure being required for each security level. The goal was also to allow coalition network access via networks operating at national security levels.

Task 4 has explored, specified, and demonstrated mechanisms for automatic management services and service levels in coalition networks. The main challenge is to automate the end-to-end management across multiple security domains during changing operational and network situations. This requires mechanisms to detect changes and operational policies that define the actions to be taken. A second area of interest has been the detection of a jammer attack autonomously per vehicle or on a cooperative basis.

Task 5 has developed an overall Experimentation Architecture for CoNSIS. This architecture defines the way in which the deliveries of tasks 1 to 4 are integrated. The task has also carried out the overall co-ordination and planning of the CoNSIS Project. It has provided reporting and dissemination of the results of CoNSIS during and upon completion of the Project. The intention has been to demonstrate technical results that can transition to an operational demonstration/scenario (outside this MoU).

2.1. Motivation

NATO Network Enabled Capability is first and foremost about achieving better interaction between the different actors involved in military operations. This implies more efficient exchange of information. Consequently, the NATO information infrastructure will consist of a federation of systems, including a plethora of different information and communication systems, as well as a mix of new and legacy systems. NATO is currently looking in two different

directions: On the one side, specifying common radio waveforms (out of scope for this project) and on the other side specifying means to interconnect different radio networks via a common backbone technology (a main topic for this project).

For Task 1, the goal of the CoNSIS experimentation was to show that it is possible to use different realization of existing, heterogeneous radios by interconnecting them via a network overlay. Transparency is important, allowing applications and core services to use the best network and physical connections to create and maintain a connection between different coalition partners.

2.2. Report Structure

Within chapter 3 the theoretical work and the results from Task 1 point of view are described. The main topics are:

- CoNSIS network architecture
- Resource management and the support of routing mechanisms
- Resource based routing algorithms
- Seamless coalition internetworks based on heterogeneous radio equipment
- Definition and usage of profiling in mobile networks
- Relation between IP based and DL networks

Chapter 4 then describes how these results are tested in practical experiments at WTD 81 in Greding. Here a realistic operational coalition scenario was used to verify how well the theoretical results can be used with today's available technical solutions to improve communications at the battlefield.

Finally, in chapter 5, recommendations regarding necessary further work, based on discovered missing elements, are given.

3. NETWORK AND COMMUNICATION CONCEPT

3.1. Network Reference Model

This section gives a brief overview of the Network Reference Model described in "System and Experimentation Architectures - Version 1.0" [5]. Readers that are familiar with the model are encouraged to skip this section.

The CoNSIS reference model consists of a core network to which user domains are connected via IPsec crypto devices. The core network itself is composed of a number of interworking networks operated by different administrative authorities. Figure 3-1 shows the main elements of the CoNSIS architecture.

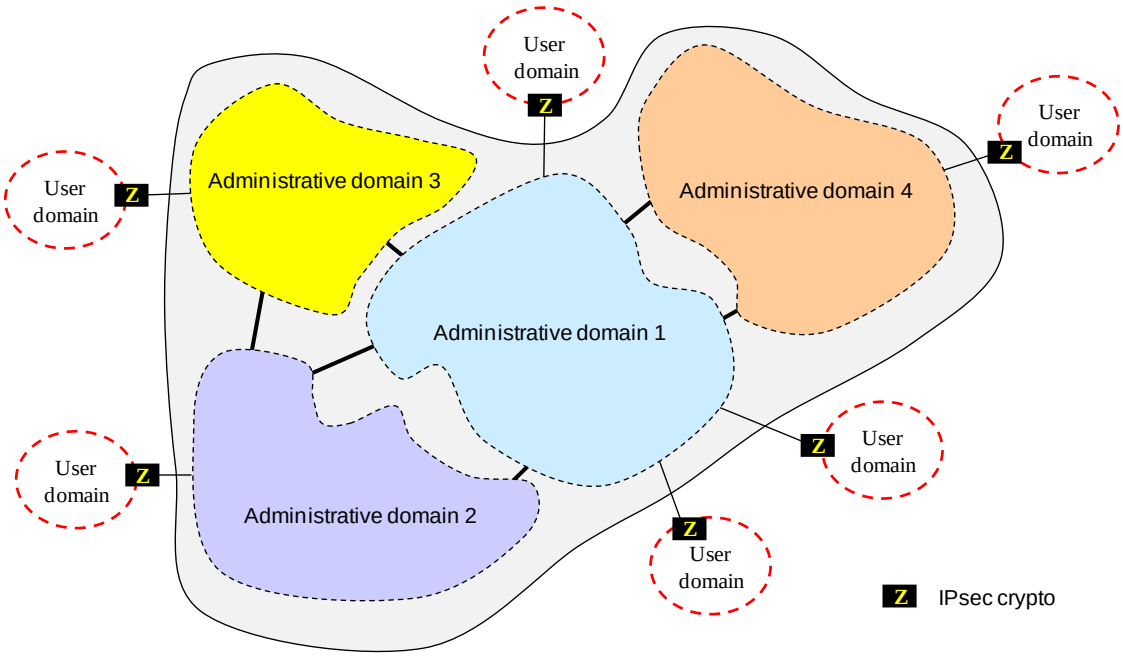

Figure 3-1: Administrative Domains

This architecture is close to the Protected Core Network (PCN) [2] approach.

In the PCN concept, secure red networks are represented by the Colored Clouds (CCs), while the black transport network is represented by the Protected Core which may consist of several Protected Core Segments (PCSs). Two interfaces are key to the PCN concept. PCN-1 is the interface between different PCSs, while PCN-2 is the interface between PCSs and CCs. The usage of the interfaces are enforced by so called E-nodes The CoNSIS network architecture is based on this concept, but the two reference models are not identical. In particular, CoNSIS administrative domains are not assumed to have exactly the same functions as PCSs regarding e.g. security protection and the management of SLAs. The administrative domains interwork via interfaces which are not supposed to have the same features as the PCN-1 interface. Likewise, the generic interface between CoNSIS user domains and the core network is not necessarily compliant with the PCN-2 interface.

In order to reflect the above-mentioned divergence, objects of the CoNSIS reference model are given names intentionally different from their PCN counterparts (see [2]):

- The core network (counterpart of the PCN protected core) is referred to as the **Transport Network** (TN).

- The TN is a collection of interworking **Transport Network Segments** (TNS) (counterpart of PCSs), each TNS being defined as a set of network elements under a single administrative authority. A segment administered by a national authority is referred to as an N-TNS while a segment administered by the coalition is a C-TNS.
- User domains are referred to as **Colored Enclaves** (CE) (counterparts of coloured clouds), separated from the TNS by IPSec. A CE can be embedded within another CE; in that case it is called an **Inner Colored Enclave** (ICE).

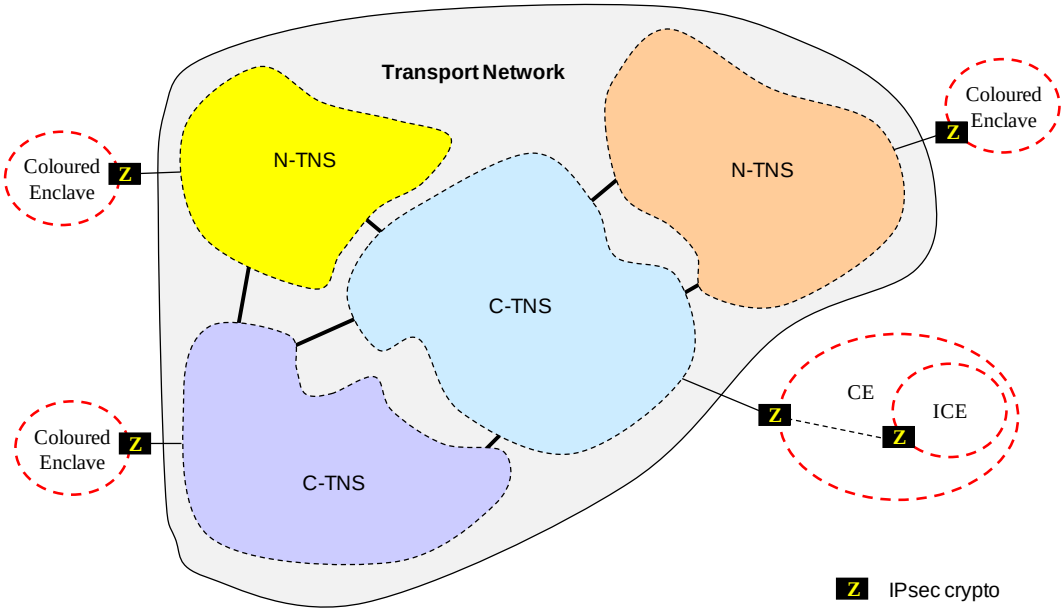

Figure 3-2: Network Segments and Colored Enclaves

The model shown in Figure 3-2 has to be translated for CoNSIS purposes into concrete details:

- Each of the TNS was realized e.g. by nationally deployed networks and common coalition networks. The convoy described in chapter 4 represented a C-TNS with radio equipment from different nations. . To avoid interoperability problems, some basic agreements were used (e.g. common addressing scheme) to allow a seamless interconnection of the national TNSs and the coalition TNSs.
- The technology within a mobile TNS was realized using several homogeneous radio networks (e.g., IABG HiMoNN and KDS WM600) From an architectural point of view, the number of radio networks present in the TNS is not relevant, as a TNS offers a connected network service to the outside, regardless how it is organized internally

This means, that CoNSIS operated all wide area connections as a black network, all user data / information is above the IPsec crypto.

3.2. Resource Usage in CoNSIS Network Segments (QoS approach)

Used (radio) equipment from each partner in CoNSIS is typically heterogeneous, based on the available nodes being offered for coalition purposes. To provide a transparent network connection for any user, independent of nationality and location within a coalition network, it was necessary to select a Quality of Service (QoS) approach, which describes the capability of a radio node independent from a specific manufacturer.

The System and Demonstration Architectures [5] aims to demonstrate, among other mechanisms, end-to-end QoS support. For this purpose, a set of QoS-classes and their associated properties are defined in this document. A strategic high capacity backbone network and a highly mobile wireless network at the tactical edge will not be able to support the same level of QoS for all application types. However we believe that one set of QoS-classes should be defined that is valid for the complete military network. Some network types must then be allowed to support only a subset of the complete list of classes, or support the classes but with less rigid maximum and minimum limits for the QoS-class properties. This design facilitates end-to-end QoS throughout a coalition network when all network segments have a common understanding of what a specific QoS-class tag represents, compared with a situation where the different network types operates with proprietary QoS-classes, and QoS-class translation must happen between networks.

DiffServ-based mechanisms are combined with Multi-Topology Routing to react specifically to requirements from tactical mobile (radio based) networks. The QoS parameters are then used to select a specific routing topology. The QoS parameters used in CoNSIS are not limited to ground based tactical radio networks, but also other networks in the tactical arena, like tactical SATCOM.

The QoS classes being used in CoNSIS are based on a reference document from NCIA [7].

SBC	Service	One example of mapping between CoNSIS services and the SBC		DSCP	
NETR	Network Infrastructure	- Routing (e.g. OSPFv3-MT, BGP, OLSR) - Management, ICMP Error Messages - TIBER Auto detection of classified enclaves		CS6	110000
OAM	Network Management	- Security management		CS2	010000
SIG-T	Call Signaling	- VoIP signaling (SIP) - Notification Management Service - Service Discovery Service		CS5	101000
VOICE	Voice		F		101010
			P		101100
		- MELPe	R	EF	101110
VIDEO	VTC		F	AF41	100010
			P	AF42	100100
			R	AF43	100110
STREAMING	Streaming media		F	AF31	011010
			P	AF32	011100
			R	AF33	011110
LDELAY	Low latency data	- Operational Alarm Messages - NFFI Blue Force Tracking Service	F	AF21	010010
		- Chat Application	P	AF22	010100
		- Network Services (e.g. DNS, DHCP)	R	AF23	010110
BULK	Bulk	- Image messaging service	F	AF11	001010
			P	AF12	001100
			R	AF13	001110
NORM	Best effort	Other applications		BE	000000

Table 3-1: QoS-classes used in the CoNSIS field experiment

Tactical radios use a wide range of transmission technologies, thus showing large variations in throughput, transmission delay, round trip time, jitter, etc. Based on lower layer protection (e.g., FEC or ARQ) bit error rate and loss ratio vary. These mechanisms again influence delay, jitter and round trip time. Thus mapping Service Based Class (SBC) and IP Military Precedence Level (MPL) onto the best MAC/PHY radio profile (and/or the most suitable waveform if several are available) is not a trivial task. In some cases the radio will not be able to support a certain SBC at all (e.g., an HF radio will always show large roundtrip times and is thus not suitable for traffic requiring short round trip times).

3.3. MT-supported QoS architecture

One of the mechanisms proposed by CoNSIS to improve resource utilization in a heterogeneous military mobile ad hoc network (MANET) is the Multi Topology (MT)-supported QoS architecture. The architecture as well as the test results from the CoNSIS MT field experiment are described in detail in [8]. In the following we give an overview of the purpose and benefit of this architecture.

To provide a reliable network for different operation types and in varying terrains, a tactical mobile network infrastructure must consist of a variety of wireless network types, e.g., long-range communication for reach-back connections, and a higher bandwidth network for local communication. A single transmission technology, e.g. a VHF network, will not be able to support all communication types and bandwidth requirements. This combined with the fact that the different nations usually bring national radios manufactured by different vendors to the battlefield result in a situation with a large number of different, non-compatible radio systems present in the mission network. One aim of Task 1 was to be able to combine all available radio systems in an operation to provide an efficient, common network for coalition use.

This gives the operator a single entry point to the complete heterogeneous coalition network. A common network will be better utilized, and multiple transmission technologies and routing paths will also improve the network reliability by providing alternative routing paths during e.g. jamming attempts. The resulting coalition network will consist of radios which have large variations in properties such as transmission capacity and range. It is however challenging to administer, admit, and route traffic flows in these networks.

In a mobile tactical network there will in most cases be limited capacity. It is therefore crucial to support prioritization of mission critical traffic. It is also desirable to use the tactical network in the most optimal manner and thus make sure that only traffic that has a high chance of reaching the destination is admitted into the network. One way to increase the network throughput is to take advantage of parallel paths in the heterogeneous network and efficiently exploit all bandwidth resources.

Since the transmission means used in tactical networks have large variations in capabilities, CoNSIS finds it advantageous to define multiple routing topologies in the network in order to support different QoS classes. These topologies are then used to ensure that data packets are only forwarded on topologies with sufficient capacity to support the requirements of the data-flow. In this section we describe an architecture where we combine Multi-Topology routing (MT-routing) [9], [10] and traditional DiffServ-like [11], [12] mechanisms to utilize all available transmission means in the tactical network and increase the robustness of the network. We name this design "MT-supported QoS architecture".

3.3.1. Multi-Topology routing

A traditional link state routing protocol maintains one routing table with one entry for "the best route" to all destinations in a network domain (or several of the best routes for load balancing purposes). The best route is calculated based on the chosen metric, e.g., shortest path first (SPF) or lowest cost, where the cost parameter can be established based on any set of link parameters.

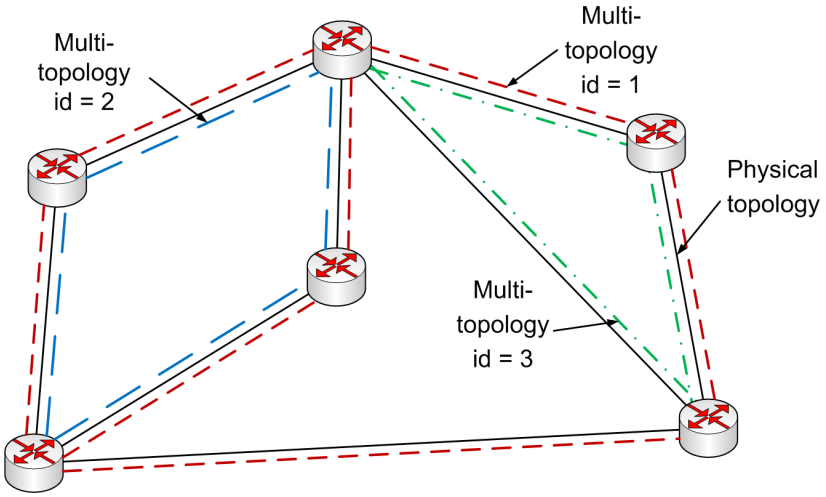

Figure 3-3: This figure shows a network with three different topologies

A Multi-Topology routing protocol maintains several topologies within the network domain at the cost of a few extra bytes in the routing packets. Each topology spans a subset of the physical topology. A shortest path first calculation (other metrics can be used if available) is performed for each topology to discover the best routes within the topology. The cost of one link can be set different for the different topologies. Only the links belonging to the actual topology are included in the calculation. The results of each SPF calculation are stored in one forwarding table for each topology. In Figure 3-3 we show a network where three topologies

are defined on top of the physical topology. A number of topologies can be defined on a single physical link. All the physical links in the domain must be part of the default topology. The default topology is used for routing traffic and ensures that routing information is flooded to the whole network.

During network configuration, topologies can be tailored to represent many different purposes. MT is used for the following cases in CoNSIS:

- Topologies can be created that have sufficient (maximum) resources to support a certain QoS class, or multiple QoS classes.
- A specific topology can be created to be used for transit traffic through the network.

MT-routing is a very useful tool that can be used to solve many situations where a certain end-to-end behavior is needed in tactical networks. This comes at the cost of a more complex network configuration.

3.3.2. Interaction between a Multi-Topology routing domain and a Single-Topology routing domain

The MT-routing specifications both describe interaction with Single-Topology routing (ST-routing) through the default topology *main* (designated table 0 in MT). We do not view this approach as suitable for a mobile military network. The main reasons for this are:

- The default topology covers the entire network and does not take into account transmission characteristics for the respective links.
- For IPv6 the routing protocol load would be close to doubled, since the layout structure of the MT routing protocol messages are incompatible with standard messages for the protocol without MT support. In order to obtain compatibility with ST-routers, the MT capable routers have to transmit both encodings.

Furthermore, there exists no description of how to import routing information from an adjacent ST-routing protocol into the MT-routing protocol, without using the default topology. This can be regarded as a weakness in the specification, since it will only be the high capacity topologies of the MT-routing domain that are usable for connection with external ST-routing networks. The default topology normally does not have the ability to differentiate between traffic. In the CoNSIS project we wanted to have the interaction both between the MT-routing protocol and an exterior gateway protocol (EGP) as well as an interior gateway protocol (IGP).

We implemented a very flexible solution for CoNSIS where we allowed import of routes from connected networks into (none or) any number of topologies. This involves both redistribution of the adjacent ST-routing protocol information into the different topologies, and a copy of the ST-routing information made available to the MT-routing forwarding tables. Since redistribution only provides the routing information to neighboring nodes and not to the unit itself, this has to be a copy. The import and redistribution mechanism uses the *main* routing table as the source for the routes.

We provided the same flexibility for export of routing information from the MT domain to connected ST domains. It is possible to make routes available from none or any number of topologies via the *main* routing table for redistribution in connected ST domains.

It should be noted that some planning is necessary to use the flexible mechanisms for import and export of routes in the best manner. One should be careful not to (by accident) import routing information from a network (e.g., network 1) into other topologies than the one that is

made available for redistribution into network 1. If this mismatch happens there will be asymmetry in the network routing information and some traffic will only be able to flow one way. However, in some cases this mismatch in routing information can be the correct configuration. E.g., in a QoS architecture there could be a policy saying for example that non MT-routing networks should be given the same or more routing information than the MT-routing network. Traffic with QoS tags that cannot be supported by the current MT-routing network will then be dropped at the entry point to the disadvantaged mobile MT-routing network.

3.3.3. QoS architecture

The CoNSIS QoS architecture for the network layer in the land mobile network divides the QoS operations in two functional entities:

- One entity that supervises the network resource management. This mechanism is needed at the ingress of the network.
- One entity that handles network congestion, packet forwarding and packet prioritizing required by the different data flows. This mechanism is needed in all forwarding elements in the network.

In CoNSIS we propose to use MT-routing to support the entity that supervises the resource management of the network. In the MT-supported QoS architecture, we configure and maintain several network topologies that each spans a subset of the physical topology. Each topology has its own forwarding table that is used to forward packets classified as belonging to that specific topology. If a destination address is not available in the forwarding table associated with the QoS class, then no path exists in the network where the specific QoS class is allowed to be transported. Thus the flow should not be admitted to the network. Traffic is stopped at the network edge and not (in a worst-case scenario) forwarded through the entire network just to find that the last hop to the destination is a link not able to support the flow's QoS requirements.

When there is a route to the destination in the correct topology and the traffic flow is admitted to the network, the DiffServ mechanisms come into play. A queue hierarchy and packet scheduling mechanism prioritizes the sequence of transmitted packets on each interface. For each network interface we also define a traffic shaper, whose purpose is to keep the traffic transmitted on each link below a certain threshold, to avoid network congestion. We use queue and scheduling tools to tailor the queue to the requirements of the associated QoS class, and to implement packet scheduling for traffic priorities. Queue length, head/tail drop and drop-precedence are important queue parameters, while the packet scheduler could be designed for a strict priority scheme or a situation with more fairness in the scheduling process.

3.3.4. MT-routing SW

We have implemented the Multi-Topology support for OSPFv3 and OSPFv2, as well as “MANET OSPFv3 MANET Designated Routers (MDR)” [13] into the Vyatta 6.3 (Napa version) [14] Linux distribution. This is based on the Quagga [15] open source routing application running on a Debian system with Linux kernel 2.6.37 (ATOW). The MANET OSPFv3 base protocol was fetched from [16]. The router implementation allows easy configuration of OSPFv2-MT and OSPFv3-MT information. Metrics can be set up for each topology on each interface. The Linux platform is set up to utilize multiple forwarding tables and Quagga's interface towards forwarding tables in Linux has been adjusted to allow the use of multiple routing tables. In addition to OSPFv2-MT and OSPFv3-MT routing, the implementation also supports configuration of static MT-routes. A flexible import and redistribution of routes from

other routing protocols via the main routing table is supported, as well as customized export of MT-routes to the main routing table to make the routes available to other routing protocols.

The target network for MT-routing in CoNSIS was a very heterogeneous MANET. Standard OSPFv3 is not suited for such networks with a high rate of connectivity changes. The MANET extensions to OSPFv3 on the other hand, can better support this network type. For this reason we implemented MT support in the MDR extension to OSPFv3. Unfortunately, due to experienced instabilities in the MDR OSPF protocol base, standard OSPFv3-MT was used in the CoNSIS field experiment.

Details of the MTR concept as used in the CoNSIS experimentation are described in chapter 4.2.1.

3.4. Concepts of interconnecting various heterogeneous networks into one common seamless one

The following section describes an approach for interconnecting mobile nodes on the battlefield. The main focus within CoNSIS was to use existing non-interoperable radios and still allow seamless communication between all users regardless of what radio they are connected to.

3.4.1. Concept of heterogeneous radio systems within a common, seamless mobile network

One way to integrate heterogeneous networks is to build a common IP overlay on top of all radio networks. This implies that every user within the mobile network (and, of course, within the fixed part of the network compound) can freely address any other user within the same network compound.

It is necessary to have routing across all the different network segments so reachability information is exchanged between them. This can be organized either in a flat common segment or hierarchically ordered.

The disadvantage of this approach is, that for a number of nodes within a single network segment, more than one radio must be installed (in case of the CoNSIS experimentation in June 2012 up to three different radio were installed in one car). This costs more space and energy and therefore such a solution is not recommended for single soldiers.

To allow seamless routing across various radios, a common routing protocol is recommended. In case of the Greding experimentation, some radios (e.g. HiMoNN) were using OLSR on the lowest routing level. As a common solution (across several radio segments) OSPF MDR (RFC 5614) was used (on top of the radio-internal routing protocol), but other pro-active routing mechanisms are also possible. If there is no way to operate one single routing domain, some kind of cross border routers (like BGP) are necessary, but then an automatic integration of formerly independent network segment into one common segment is more problematic.

The second approach for operating such a model is the handling of prioritized traffic within mobile networks: As described in chapter 3.3, the generation of logical network overlays (as it is realized using MTR), needs a common understanding and usage of the radio parameters, to allow the generation and maintenance of a homogeneous path through the network. These topologies (e.g. high bandwidth, low delay, or similar) can be defined across a number of (national) radio segments, if a common understanding of the parameter classes is there in all segments (in case of the Greding experimentation, the real throughput for various radios differed significantly, e.g. up to 11 Mb/s for HiMoNN and up to 2 Mb/s for Kongsberg. Independent of these conditions, a high bandwidth class was defined for throughput up from 500 kb/s.

3.4.2. Minimum requirements for radios in an seamless mobile network

The radios being used in the Greding experimentation, were designed and implemented independently, as there is no common guideline for the operation in coalition networks available, e.g. from NATO.

Most of the radios today with a network protocol stack offer an own, internal routing protocol. These routing protocols are normally adapted to the specific needs of the underlying radio and quite often not interoperable with routing protocols of other vendors. To avoid such a non-interoperability solution, these routing protocols can be used within a single, homogeneous network segment, but for inter-segment purposes, a common routing protocol is required, in addition to (running on top) or instead of the local routing mechanism (if it is possible to de-activate a local routing protocol within radios by simple configuration).

Besides the common understanding by using an overall unicast routing protocol, the parallel specification of a multicast routing mechanism is of a similar priority. At least in tactical operations, a one to many communication is quite common. To support this, a routing mechanism that supports high mobility and varying channel conditions is of high importance. Because of this dynamic environment, a classical membership of end nodes within multicast groups is difficult to support. Therefore other approaches to get an efficient multicast communication running, are necessary. The solution within CoNSIS was to use efficient optimized flooding mechanisms for multicast traffic (e.g. by using Simple Multicast Forwarding, SMF).

An additional problem may arise in the area of traffic control, when interconnecting different network segments. Again, inside a (national) network segment an own type of traffic control may work. To get it running across various segments, an overall traffic control is necessary, therefore the function TC (Traffic Control) from the Linux route-2 environment in combination with the MTR routing topologies was used in the CoNSIS experimentation.

To allow the integration into a heterogeneous network, the following elements were used as appropriate:

- Ethernet interface for the local connection of a radio to the overlay router
- A common routing protocol running on the overlay (e.g. OSPF MDR, RFC 5614,)

Beside these two requirements, a set of highly recommended conditions should be fulfilled:

- The physical description of conditions between communicating radios should be reported automatically from the radios towards the interconnected routers (e.g. using PPPoE from chapter 3.4.3.2). Based on the local PPPoE parameter values, radios may define an own flow control (peer-to-peer) across the common radio link.
- The configuration of each radio node should be harmonized: If some radios are using large input buffers to overcome temporary radio disruption and other ones not, then this will influence the performance of the overlay routing protocol (for details, see chapter 3.4.3.4.2). A small buffer should be configured in each radio node for the traffic class that the overlay routing messages are tagged with. If the buffer used for the routing signaling messages are large, the efficiency of any pro-active (and, indeed for re-active) routing mechanism is reduced.

3.4.3. Routing strategies

When creating an overlay network, based on various sub network technologies, an urgent question to be solved is which routing strategies should be used.

The approach in Task 1 was, not to exclude any existing radios from being included into the overall network, which means, that a variety of available bandwidth from a very low number of kbit/s up to several Mbit/s will be available.

Especially in the area of very low throughput, the routing mechanisms consume for own purposes a significant part of the available bandwidth. Therefore, for the limitation of the so-called control information, the selection of the most efficient routing strategies should be done quite carefully.

On the other hand, the connectivity information within a tactical network should not be limited. For the reachability of remote end systems, there should be enough information available at a sending node, avoiding burst behavior at the beginning of any communication before exchanging user related information.

Having these considerations in mind, it was decided within the CoNSIS project to use pro-active routing mechanisms which provides ant any time connectivity information to the users about remote end systems.

As available algorithms, which are stable enough in the standardization, the following were selected:

- OLSR (optimized link state routing)
- OSPFv3 MDR (open shortest path first)

Both algorithms are optimal for the usage in a radio environment for several reasons (see below the considerations on MTR), OSPF was selected as the preferred one for unicast routing within tactical domains.

Nevertheless, the amount of control information to keep alive the information about connectivity within the network is still a problem in such an environment. Especially in multicast protocols with dynamic membership management, the amount of control information is growing dramatically. Therefore CoNSIS was looking for pro-active multicast routing algorithms with limited amount of control information.

Especially in tactical networks with a changing number of active nodes inside a radio network, a membership management cannot be implemented in a bandwidth efficient way. Therefore CoNSIS proposed not to use an algorithm with membership management. Instead an algorithm which abstains from membership management was selected. The so-called Simplified Multicast Forwarding (SMF), a development from NRL, was chosen [31]. This mechanism uses the broadcast behavior of radio networks to do optimized flooding in the network with the multicast traffic by avoiding loops between routers. If it is coupled with the OSPFv3 MDR routing protocol, SMF can use the MDR algorithm to calculate designated routers for flooding forwarding. This behavior is acceptable in a limited (radio based) network, as the number of nodes without multicast members is quite small.

As SMF was verified as working well in a radio environment, the mapping of this mechanism into backbone networks was a problem. In more fixed network, a flooding behavior is not recommendable. Therefore a mapping between SMF and other multicast mechanisms was necessary.

As CoNSIS was using in these backbone networks more standardized multicast routing (PIM-SM, IETF RFC 4601), a workaround was necessary to combine both algorithms by declaring a SMF domain as a member in PIM-SM. This way, it was possible to exchange multicast traffic in both routing domains.

The last aspect for the consideration on routing strategies was the consideration of resource aspects. As radios with significant difference in throughput were used, it is not worthwhile from an application point of view to use any network connection. In contrary, some applications will require a minimum bandwidth end-to-end to have an acceptable behavior for all users.

To provide from a network point of view enough resources, the concept of MTR (multi-topology routing) was used. Here, several logical routing topologies are created, based on specific availability of resources, which will lead to different routing of IP PDUs across a network, based on specific QoS values being assigned to these PDUs.

Currently, the MTR concept is realized by THALES Norway in combination with OSPFv2, OSPFv3 and one MANET extension to OSPFv3 (MANET Designated Routers (MDR) RFC5614). (Due to instabilities in the MDR source code, standard OSPFv3 was used in the CoNSIS field experiment as described in chapter 4). MTR generates for each routing topology configured on a node, a separate routing table in the (Linux) kernel. When a route is available to a certain destination in a specific routing table, then a path exists to the destination where the QoS parameters associated with the specific topology can be supported. It should be noted that MTR is not aware of the load on the network, thus a path might exist, but it might be busy. Currently Multi Topology routing is only implemented for OSPFv3 and OSPFv3 MDR thus this was the major argument for using the OSPFv3 family as the common routing protocol in the routing overlay.

3.4.3.1. Prioritization in Radio networks

The prioritization mechanisms used in CoNSIS are in principle located at the internetwork routers, outside the radios. Therefore theses routers are responsible for forwarding and organizing IP PDUs in a radio network. The only chance for radios to influence the prioritized forwarding of PDUs is to modify the router decision by reporting back conditions about the real radio link from the radio towards the router.

This report also includes the hardest way of a link description, radio silence. This operation, normally ordered in case of a special military scenario, can be described in terms of link parameters with extreme values (e.g. throughput 0 kb/s or delay endless).

In consequence, the prioritization is not a task for the used radios, independent whether radios with significant buffers were used or not (in case of buffered radios, different buffer lengths were used, short ones for buffering control (routing) information and longer ones, buffering user information; while short routing buffers seems to be acceptable, the queuing of user information should normally not the task of a radio, but of the attached routers or end systems).

3.4.3.2. Resource determination in Radio networks and integration into the routing process

It is still a great challenge in radio based networks to get reliable information about a (radio) link in order to adequately regard it during calculation of routing metrics. Metrics about a link and its current situation and historic development is not only necessary for QoS but also vital for reliable and fast routing decisions. This is especially true in a MANET.

Current radios / modems typically provide an Ethernet interface to connect the radio / modem to the routers or terminals behind. From the standpoint of the router this link is usually a good quality copper link with high bandwidth - no matter what the radio link behind can serve. Of course you can easily take the lower link rate and quality into account by putting an additional but static weight to the link. However, such a configuration cannot take dynamic situations and changes into account - a very important capability for MANET environments. Another

big issue is that technologies that propose to solve such issues are usually proprietary, not compatible with each other, limited to a specific range of radio environments, difficult to integrate in existing devices and cumbersome or complex in architecture.

The approach that has been investigated in CoNSIS is based on a well deployed and tested technology: PPP and its enhancement PPPoE. One can say that PPP is not a new technology but in fact it is still very much present today - in all kind of network environments. It should be noted that the technology (PPPoE) and its extension defined in RFC5578 "PPPoE Extensions for Credit Flow and Link Metrics"[RFC5578] is not used in the way PPPoE was intended in the first place. However, the good part in reusing technologies is that usually these technologies have already proven their capability, are tested and usually accepted and implemented widely. The best example for day-to-day reuse that improves more and more are either nature itself or the well-known LEGO bricks.

It has to be mentioned that there is a very promising new approach emerging, a more native and improved solution compared to RFC5578. It defines a new protocol and is not anymore re-using PPP/PPPoE however providing the same capabilities. It makes use of the protocol language defined in RFC5444, which has been developed to define / develop MANET protocols. This new approach called "Dynamic Link Exchange Protocol"[DLEP] appears to become tightly related to MANET (very likely OLSR). However, it makes no sense to base any implementation on it, yet, as this approach is still in early draft status and a matter of constant change. The interested reader can take a look at [38] where PPPoE, DLEP and a third radio to router interface R2CP is compared and analyzed for tactical networks. This topic is also being discussed on the IETF Manet working group [IMANET].

This paragraph describes a technical solution for a RFC5578 conform implementation. It covers the client / radio part which will be based on the existing RFC4938/5578 open source code for Linux/Unix platforms available at [SF4938]. This client code is tested with Cisco's RFC4938/5578 implementation (see [C-PPPOE], [R2RC]).

Furthermore it covers a server / router implementation for Linux/Unix platforms. This implementation covers the RFC5578 part a) towards the client / radio and b) towards the routing engine (via a generic API) as well as an adjusted OSPFv3 routing engine (based on the routing framework [VYATTA, QUAGGA or any other]). This server / router implementation will be tested against the Cisco IOS implementation in order to reach compatibility and allow for an open source alternative. Optionally an adaption to OLSR will be considered. However, this depends not only on the results gained by the implementation described here and the feasibility for such an approach, but also if alternatives like DLEP will promise better results (given that these are in more stable state).

This chapter summarizes the credentials of the technical approach defined in RFC5578 and relevant information of Cisco's implementation as it could be gained during evaluation. Therefore, the following can and should be seen as a reference (or cheat sheet) for the later description.

3.4.3.3. Network virtualization through using a tunneling concept

The protocol profile being used in CoNSIS may at first seem a little bit curious: An OLSR/OSPF MDR is topped by a full meshed tunnel, where an OSPF-MT is running again as a higher routing entity.

This solution was selected because of the following reasons:

- OLSR/OSPF MDR was implemented in all used radios as a default routing mechanism

- While HiMoNN and Kongsberg WM600 were using **primarily** IPv6, Flexnet was only IPv4 capable. Therefore a full meshed model with GRE-tunnels and ip6ip6-tunnels was used, offering to the top side of the network profile a common IPv6 interface, while towards the radios different IP versions were used)
- The multi topology approach is currently only defined in combination with OSPF (an extension to OLSR is in principle possible, but not yet specified)

To allow a seamless operation of OSPF-MT, using IPv6 across a heterogeneous radio network, GRE and IP6IP6 tunnels were used between all active radio nodes with a wireless hop limit of 1 (to enforce a correct count of wireless hops in the overlay routing protocol metric). This GRE tunnel allowed the operation of OSPFv6 MT over radios with IPv4. The GRE tunnel also allows the forwarding of multicast IP packets (again, using the hop limitation of 1) to distribute IPv6 multicast packets across any kind of radio. IPIP tunnels were used over the IPv6 capable radios. A packet wrapper was created for CoNSIS to support forwarding of multicast traffic over these tunnels.

The disadvantage of this concept is, that the maximum number and addresses of all mobile nodes must be known in advance. No additional node with an unknown IP address can be integrated into this full meshed overlay. A smaller number than the maximum is no problem, as the specific tunnels to this node will remain inactive.

3.4.3.4. Network Support for upper layer requirements

The network concept being operated in CoNSIS uses a black network connection between all active network nodes, whether they are located in mobile ore fixed networks.

The security architecture (for details, see Task 3 final report) assumes a strict, node oriented protection at network level. To support an ad-hoc behavior consequently at all protocol level, the IDP/TIBER implementation from the INSC project [39] was used.

Main element of the ad-hoc behavior of IDP/TIBER is the periodic exchange of Hellos, looking for potential counterparts within the (tactical) network.

The Hello-messages being sent out can be used as a trigger to stimulate the initialization of upper layer protocols (e.g., the SyncD synchronization service, as described in the Task 2 final report.

CoNSIS started from the beginning of the project using this Hello, but from an architectural point of view, the Hello mechanism was repeated at application level at a later project period. The resulting service providing this ad-hoc behavior, was then called Generic Advertisement of Applications (GAA). The usage of this service is explained in the Task 2 report, too.

3.4.3.4.1. Multicasting in radio networks

Radio networks are broadcast capable by definition. Therefore, for tactical usage, a radio network should be able to use this behavior up from the beginning.

The main difference between fixed networks and radio based (ad-hoc) networks is the probability that a connection exists between two nodes. In fixed networks, the probability for a connection is nearly 100 %, in tactical radio networks, based on the operational scenario, much less than 100 %.

For standard group communications, routers must know where active group members are placed to forward an IP PDU towards this end point.

In tactical radio networks, end systems and routers are quite often identical. Connectivity to neighbored nodes will vary significantly over time with the consequence, that such a node

may be available as a router (for multicast traffic) and at the same time may be member of a group.

For nodes, temporarily not connected to a network, it makes normally no sense to forward multicast PDUs towards their destination, as the PDU will be destroyed somewhere within the network. To avoid this un-necessary forwarding, a membership management protocol is used in fixed networks to manage the membership of each exiting (or not longer visible) node.

As in tactical networks the radio network connections will change its status quite often and unexpected, this group membership traffic will increase dramatically.

To avoid this behavior, CoNSIS chose a multicast protocol without any membership management: Simple Multicast Forwarding (SMF), rather than a full membership management multicast routing protocol (e.g. PIM-DM). SMF floods the network with multicast traffic towards any existing end system, independent of whether this end system has announced a membership to a group or not. The main purpose of SMF is to avoid loops within the network for unnecessary retransmission of traffic over the same link several times. SMF can also optimize the flooding process by choosing a minimum set of forwarding nodes to cover all two-hop neighbors. OLSR's MPR[18] and OPSF's MDR[13] are two algorithms that can used by SMF to calculate the necessary forwarding nodes.

This multicast routing service was used by Task 2 e.g. by WS-Discovery and by Task 3 to support IDP/TIBER.

Unfortunately, SMF and PIM-SM are not interoperable. Currently it is not specified, how a multicast routing protocol with group membership management can interoperate with a multicast routing protocol without group membership management (Open question for standardization).

As a workaround in CoNSIS, an administrative entry was done in the PIM-SM configuration in a way that the prefix address of the mobile segment was manually added as a member into the PIM configuration. With this trick, multicast traffic can be exchanged between a fixed and a mobile network. The disadvantage is that mobile networks must be handled as leaves in the complete routing tree and cannot be used as a transfer segment in a network compound.

3.4.3.4.2. Mechanisms for congestion control and harmonization between various mechanisms

The conditions in radio based networks diverge severely from those in fixed networks. Although using pro-active routing protocols, it costs significant time to report changes within the network towards the end users. As a consequence, traffic will be forwarded to a foreseen end system on routes being known to the sender, but not reflecting the reality inside the radio network.

As a consequence, traffic will arrive at a node, where forwarding to the next hop is not possible and, in addition, no alternate route will be available via different nodes.

Some vendors (e.g. Harris within the AN/PRC 117) have chosen a way to overcome this problem: IP PDUs which cannot be forwarded under current conditions (e.g. broken link), are stored temporarily within the node. This behavior is known as buffering nodes.

When a new route to the destination is detected, the buffered IP PDUs are sent out, so, from the point of view of the receiving end system, there is no traffic loss, only an additional delay.If a radio is configured to buffer packets for a certain time in the situations when a route to the destination does not exist, it is important that there is a common understanding of the QoS architecture (QoS classes and their characteristics) in the radio and in the rest of the network. The radio must make sure to flush the queues (buffers) for routing traffic and other delay sen-

sitive traffic after a very short delay. Other traffic classes can be buffered for a longer time. If e.g., routing messages are delayed for a significant time, these old routing messages will increase the risk of getting inconsistent topology databases and there will be more routing loops in the network.

If there is a common understanding of the QoS-classes and the buffering node has an internal queue structure for different QoS classes, then delay sensitive traffic can be identified and flushed and buffering may be acceptable (for an example of how the queue structure could look like, see [8], esp. chap. 6.3.5). Details for such a configuration can be part of a further CoNSIS phase.As a lesson learnt, it should be urgently avoided to use buffering behavior and pro-active routing behavior in parallel within the same network if the buffering is not done selectively for different QoS classes. It is better to include the real conditions of a radio link immediately into the routing decision, e.g. by reporting the appropriate QoS parameters via PPPoE directly to the router.

3.5. Improvement of Communications as a Function of Network Conditions

A way to improve communications via a network would be to keep users informed about the capability and current state of this network so they could optimize their flows and obtain the best possible quality of service.

The idea explored within CoNSIS was to include this information about the network in a data set referred to as a **Technical Profile**.

3.5.1. Contents of a technical profile

A technical profile is associated with an IP Autonomous System (AS) in the black domain of a communication system, i.e. with a TNS in the CoNSIS terminology. It contains a description of what can be expected from this TNS, including two categories of parameters:

- The TNS's technical capabilities
- The services which can be accessed via this TNS.

The technical capabilities of a black network can be described through its permanent mechanisms and through variable aspects of its behavior.

Permanent aspects are in particular:

- The list of QoS models supported by the network (e.g. DiffServ and/or IntServ and/or MPLS-TE),
- The options associated with each QoS model:
    - For example, the list of DiffServ classes of service supported, along with the corresponding DSCP coding,
    - Or for example for MPLS-TE, the list of supported RSVP-TE priorities, the meaning of the two metrics for the calculation of explicit routes, the meaning of the 32 administrative attributes (affinities) of links.

Variable aspects are mainly:

- QoS performance parameters,
- Indications about the relative stability of these QoS performances.

As a minimum, QoS performance parameters are intended to reflect the data rates the network can currently accept, the transit delay, the jitter and the packet loss rate on paths within the TNS. If the network participates in the delivery of connection-oriented services, this list can

also be complemented with such parameters as call set-up delay, call set-up failure rate or probability of an incident during a session.

There are two difficulties in representing the behavior of a network by a limited set of QoS parameters:

- The values of these indicators will depend on the class of service of the relevant flow. For example, the transit delay of an EF packet can be expected to be shorter than that of a BE data unit.
- QoS performances will be unequal on different paths.

To take into account the inevitable dissymmetry between classes of service, QoS parameters have to be specified in a technical profile for each CoS. They are thus given for each (QoS model, class) pair where for example “QoS model” identifies DiffServ and “class” identifies the EF aggregate.

The conjecture is that the problem of the inhomogeneous behavior of paths can be overcome by specifying a 3-tuple of values for each QoS parameter: the minimum, the typical (i.e. most probable) and the maximum value which can be encountered through the network. The point with technical profiles is not to give users exact and very accurate values, but only a rough idea of how their flows will be affected when they travel across a TNS. Moreover, it is expected that user hosts will have the capability to cope with a certain level of uncertainty in the technical profile thanks to intelligent strategies.

The acceptable data rates are reflected by a set of *mitigating factors* which can take values between 0% and 100%, where 100% means that the TNS is currently able to fully comply with user SLAs while a lesser value implies that the network only guarantees the delivery of a fraction of the traffic specified by user contracts.

Indications about the stability of QoS performances are intended to prompt user hosts to more or less frequently look up a technical profile, depending on whether the relevant TNS is prone to sudden behaviour changes. Three such parameters were identified during the CoNSIS study:

- A *mobility factor* reflecting the typical number of minutes after which significant changes may occur in the network topology,
- A *load dynamics indicator* which can take the values Yes or No depending on whether sudden surges are possible in the amount of traffic conveyed by the TNS (and thus cause tremendous variations of the mitigating factors and other QoS performances),
- A stress indicator which reflects the fact that the network may or may not come under heavy attack such as e.g. jamming.

A technical profile can include a description of applicative services which can be accessed via a TNS. If a SOA infrastructure is implemented, advertising this sort of information should normally be its responsibility, but in the absence of SOA functions, this can be handled by technical profiles.

The description of such a service includes:

- The IP address(es) of the server(s) from which the service can be solicited, or the multicast address of the relevant flow for point-to-multipoint services,
- The list of protocols accepted by each server (e.g. HTTP, FTP...),
- A description of the type of transaction if authentication is required prior to accessing the service (e.g. type of crypto algorithm, need for a certificate...),

- An indication of the server's current availability (Yes/No/Degraded),
- A description of the type of degradation the relevant server is currently undergoing. This aspect is service-dependent; for an email server, it can for example be that messages take twice as long as usual to get delivered.

3.5.2. Use of a technical profile

The information contained in a technical profile could be used by TNSs adjacent to a certain network to improve their relationship with this network (e.g. by limiting the traffic they send through it in transit when it is under stress). It could also be used to form the basis of some sort of policy-based management within a TNS, e.g. by allowing routers to automatically change their configuration or alter their forwarding decisions when congestions are encountered.

These are avenues which were explored during the CoNSIS project, but as the field of possible applications is extremely vast, work was mainly focused on the use of technical profiles by user hosts.

There are many ways user hosts can exploit the information made available to them in a technical profile. They all have the goal to improve the cooperation between the black network and devices in the colored enclaves, and more specifically to enhance the QoS experienced by users. To quote but the most prominent ones, these applications include:

- The choice of the most appropriate QoS model,
- The adaptation of user host communication mechanisms to current network conditions.

Whenever a network supports several QoS models, a user host has to select which one is best suited to the type of flow it is about to transmit. This requires an internal policy in the host by which it will for example determine that VoIP sessions had better be transported with a guarantee of resources (i.e. using IntServ or MPLS-TE). On the other hand, a reservation may only be compulsory if the network is constrained in terms of bandwidth, and DiffServ can very well suffice to support telephony in a broadband system. All the information necessary to make the appropriate decision is contained in a technical profile.

The adaptation of communication mechanisms to conditions currently prevailing in the network can take many forms:

- A host can select UDP instead of TCP in certain particular cases, e.g. when a heavy packet loss rate within the network will cause a reliable transfer protocol to delay the arrival of data to an unacceptable extent.
- Specific options of TCP may prove advantageous in the presence of certain network characteristics. A well known example of this sort of situation is the extension of the protocol anticipation window for communication over a satellite system, in order to circumvent the LFN effect.
- When it has to cope with a network where bandwidth has become particularly scarce, a host can skim the applicative contents it transmits, in hopes to find a better trade-off between the quality of the data exchanged and the delay after which they do get to destination.
- In the presence of very adverse transport conditions, a host can select a more robust and more economical format for its data (e.g. a particular voice codec) which, in the

same way as skimming applicative contents, will result in a better compromise for end-to-end QoS.

Finally, the black domain and user hosts can work together to reduce the amount of data transmitted through the network when it gets congested. Routers can learn via user SLAs what traffic demand is to be expected at an access point and automatically decide to enforce a limitation of user data rates based on the current mitigating factors. This form of connection admission control (CAC) with DiffServ would be an example of policy-based management techniques mentioned at the beginning of this section.

3.5.3. Mechanisms associated with technical profiles

The technical profile of a TNS is held by a repository under two forms:

- An XML document for permanent (or very stable) parameters.
- And an LDAP directory for more dynamic information and for parameters which can exist under a large number of forms (e.g. QoS performance indicators, which have to be replicated for each QoS model and each class of service).

The XML format has the advantage of being highly compatible with evolutions, and can provide users with the information they require to find out how to access the directory (e.g. which QoS models are supported). Storage in a directory avoids the transfer of a long file (and the overhead this would imply) each time a technical profile consumer wishes to look up a particular variable parameter.

Making a technical profile available as just explained is however not sufficient. Specific mechanisms are necessary for user hosts to fetch this information, to figure out network conditions when their flows traverse several TNSs, and to adapt their own behavior as a function of the information they learnt about the black domain.

And of course, the purpose of technical profiles being to make network operation more dynamic, it would not make sense if the information they contain had to be entered manually. Additional mechanisms are thus indispensable to automatically populate a technical profile.

3.5.4. Proof of concept

During national and international CoNSIS tests, all major mechanisms associated with technical profiles were successfully demonstrated. This includes:

- The storage of a technical profile in an XML file and an LDAP directory,
- The possibility to automatically and pertinently update the contents of the LDAP directory based on status monitoring information and on measurements,
- The ability of a user host to determine the list of TNSs traversed to a certain destination with the help of an AS-path responder,
- Its ability to fetch the technical profiles of all relevant TNSs, compose them and deduce from end-to-end network conditions how to adapt its own behavior to obtain the best possible QoS.

The full sequence of above-mentioned events could also be chained to illustrate the benefits of technical profiles in two operationally realistic use-cases:

- When solicited by a client, a web server finds out that the path to this host is currently congested and decides to reduce the resolution of its pictures before transmitting a HTML page.

- When it finds out that a new member connected through a narrowband network has just joined its multicast group, the source of a video stream decides to reduce the resolution of its program, or alternatively creates a new multicast stream with lower resolution for this particular destination.

In both cases, the improvement in quality of service (in terms of download delay for the web page, in terms of mere ability of the receiving user to watch the video program) turned out to be quite tangible when technical profile mechanisms were enabled.

3.6. Relation between tactical IP Networks and Data Link Networks

In the tactical area, currently two main models exist to interconnect military users: A traditional approach, using specific Data Link equipment and a modern one, using an open internetwork protocol, based on IP.

In the beginning of the CoNSIS project members assumed that a transparent network interface could be defined, allowing an ad-hoc interconnection of end systems within a DL network and end systems within an IP network. It was agreed to have such an interconnection not only on a pre-defined level, but, following the architecture for tactical ad-hoc networks, also in an ad-hoc way.

The principle assumption was that the Ethernet interface, being provided at ground terminals for DL networks, will be the main network access to the DL network from the IP network point of view.

Therefore this task was assigned to Task 1, as it was a standard network approach.

During the specification phase for such an interface, severe problems were detected:

- Ad-hoc interconnection means, that more than one network interface may exist between a DL and an IP network. This may cause a problem with the status of either the IP or the DL network: Each network may occasionally being used through two or more interfaces as a transit network (at least not acceptable for a DL network, but in many cases for a tactical IP network, too)
- Transparency includes a protected network connection between end systems both in the IP and DL network. As the whole DL networks are currently closed networks, no transparent external network interface with protection is available. In this case, a security boundary always exists with the consequence of not allowing a transparent network connection.
- The propagation of more than one interfaces from the IP network point of view raised severe problems, as the identification and naming scheme in the DL network caused a problem of unique addressing and routing in the IP network.

These reasons were assumed as so critical, that a transparent network approach was skipped and an alternative solution, message type forwarding between the IP network and the DL network was chosen: As the main information type within DL networks are well known message types, and internal and external users are communicating, using these message types, a Data Link Processor solution was chosen, translating and forwarding specific DL message types (e.g. Link 16 message types 2.2 and 3.5 as used examples during the experimentation in Greding).

DEU used for this approach a solution from IBM, the Data Link Proxy (DLP), which provided via a JMS interface transformed DL message types to a notification service as a service provider and was consuming specified message types from the notification broker (via an own subscription from the DLP towards the broker).

The interconnection with the CoNSIS environment was based on the following requirements:

- Transform and Forward TDL-Messages
  - Flight objects: Combat fighter and helicopter tracks
  - Ground tracks
  - (possibly) Stationary ground positions (facilities, troups, etc)
  - Transmitting Commands
    - E.g. land, alter course, turn around, turn left, turn right
  - Managing Subscriptions
    - Which TDL-Tracks the receiver desires to be transmitted?
  - Development and Testing Basics
    - Multilink-Processor (Link11/16/22) Simulator [virtual machine/IBM]
    - .XSD-Files of IBM and Thales
- Target:
  - Tracking of Helicopter and / or Fighter courses and visualization in an Open-Street-Map-based Presentation Tool

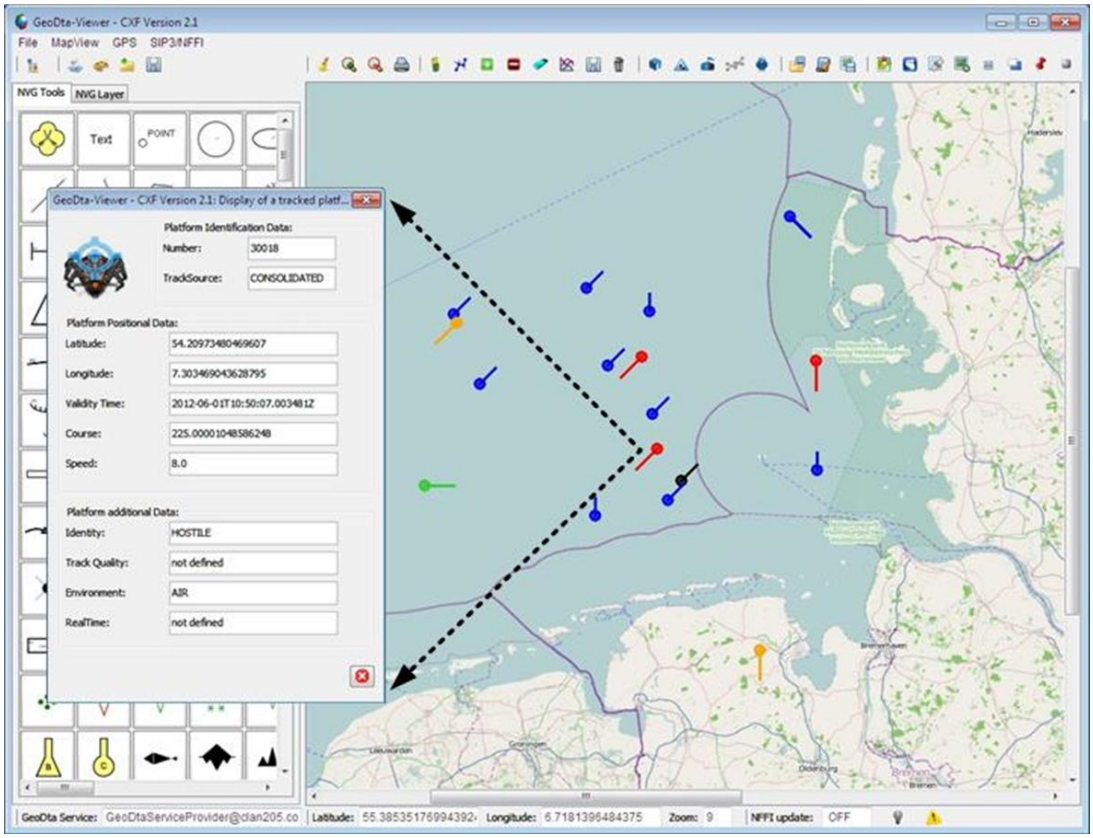

Figure 3-4: Typical operational picture in CoNSIS, based on Link 16 message type imported into the CoNSIS notification brokers

Details for the implementation of this DL Proxy part can be achieved from a separate DEU document[1].

[1] 110804_RuDi_IABG_MultiLinkProcessorService_002-english.doc

4. CONSIS EXPERIMENTATION

4.1. Experimentation Scenario

The CoNSIS scenario as depicted in Figure 4-1 is set in a country torn by civil war. International coalition troops are deployed in the country to stabilize the situation, protect the population and initiate the peace process. Larger cities are controlled by coalition forces, but the situation outside the cities is still unstable. Convoys and advanced outposts are constantly at risk of attack. The coalition troops have established an international headquarter (HQ) which has fixed network connections to several national headquarters. There are also naval forces from different nations patrolling the waters around the conflict area.

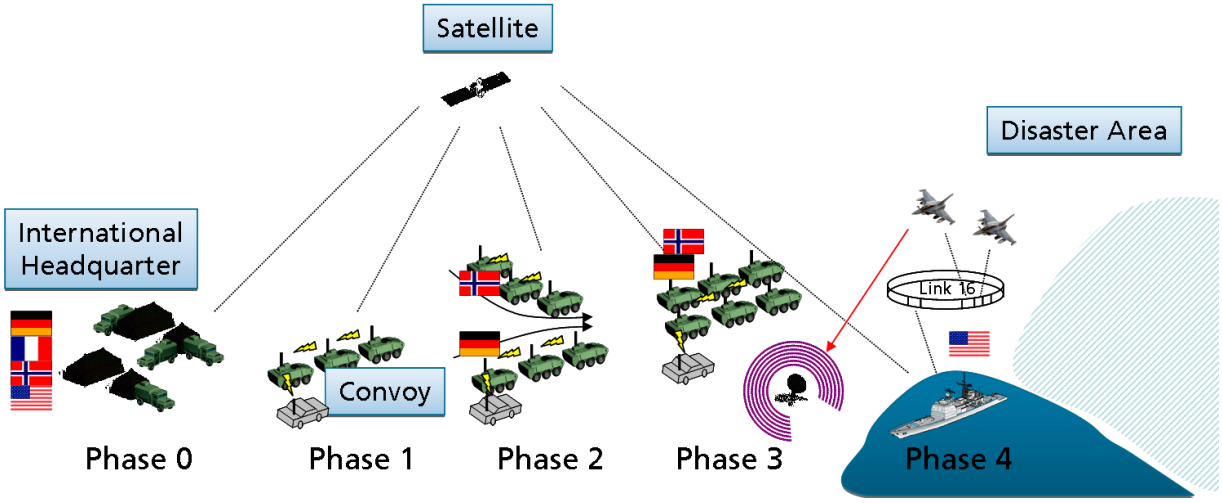

Figure 4-1: The CoNSIS network

In this situation, a natural disaster occurs in a part of the country not controlled by the coalition forces. The coalition decides to aid in disaster relief efforts by escorting the vehicles of a Non-Governmental humanitarian Organization (NGO) to the disaster site and secure the area. The military vehicles are connected by different military radio technologies operating mainly in the UHF frequency spectrum, forming an ad-hoc network. As with the naval vessels, communication with the headquarters is ensured via satellite technology installed on a few specifically equipped vehicles. The NGO vehicles are also connected to the military convoy by terrestrial radio. Shortly after setting out, the convoy is joined by a second group of military vehicles from another nation. This group uses radios not compatible with those of the convoy, but a few vehicles in both groups have radios with compatible waveforms to bridge the communication between the two groups. Following a reorganization of the network in the wireless domain, they now form a comprehensive ad-hoc network.

Making its way to the disaster area, the radio communication within the newly combined convoy is suddenly disrupted by a radio jammer. Satellite communication remains unaffected. The jamming is recognized, reported to the headquarters, and finally eliminated by an air strike.

The principle scenario layout was organized in a distributed approach:

The FRA and USA deployed headquarters were operated from their home bases, Bruz in France and San Diego in California. The network connections to these headquarters were realized using the public Internet. This is in principle an acceptable approach, as using the architecture from Figure 3-2, any transport network is per se a black one, as the user domains are

protected against these transport networks using IPsec devices. Nevertheless this approach will not be the preferred transport in real scenarios. Military long distance networks will be the favored alternative.

4.2. Field Test Setup

Experimentation in CoNSIS has a strong focus on the mobile part of the network, i.e. the convoy. It consists of three parts: NGO vehicles, Norwegian military vehicles (the original convoy), and German military vehicles (which join the convoy in phase 2). The German vehicles use three different types of radio, HiMoNN (IABG), FlexNet-4 (Rockwell Collins) and Harris (AN/PRC 117) radios. The Norwegian part uses Kongsberg WM600 radios and the NGOs commercial WLAN. None of these radio types are interoperable, which is why one Kongsberg radio is lend to the German convoy and one FlexNet-4 and one HiMoNN to the Norwegian one. In addition, at least one German and one Norwegian vehicle have a satellite connection. All UHF military radios in our scenario perform ad-hoc routing within their technology domain, which normally cannot be deactivated and provides no information about the internal topology. In addition, multi topology routing is not supported in the radios. Thus, these incompatible technologies need to be tied together in an overlay network with multi topology routing [8] support to provide some differentiated QoS in the heterogeneous mobile ad hoc network. Jammer detection is usually done by dedicated, strategically placed units. In CoNSIS, there is an experimental option of the jammed systems doing the detection themselves. To detect a jamming incident locally, information from different network layers must be correlated, which requires a cross-layer information architecture. Besides reporting the incident to the international headquarter, local measures may be taken to circumvent the jamming, such as changing frequency or modulation or reconfiguring the routing. Details for the jammer part of the experimentation are available from the Task 4 final report.

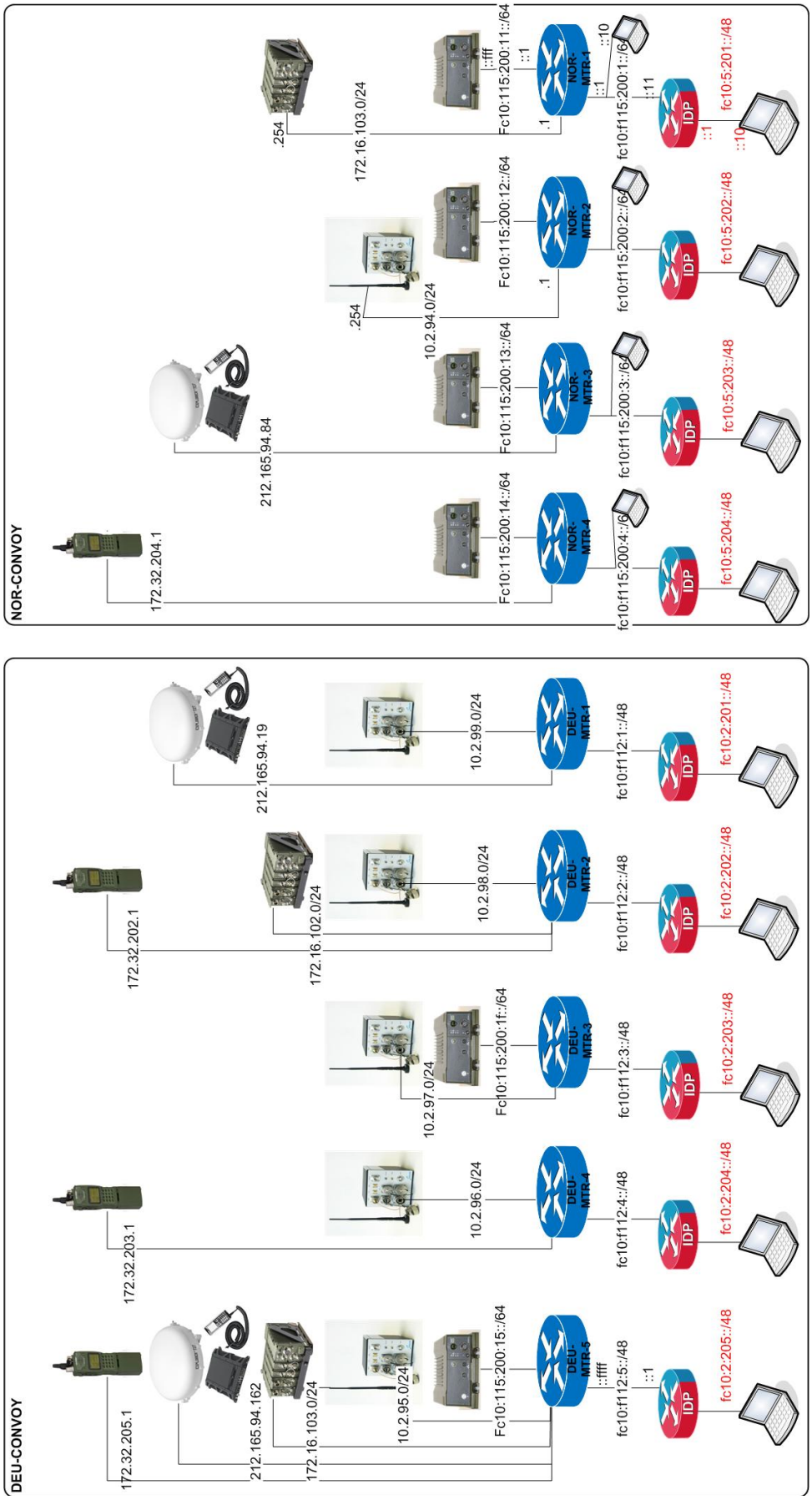

Figure 4-2: Configuration of the convoy nodes in theGreding field experiment

Figure 4-2 shows the originally intended configuration of the mobile nodes with various radios. The principle idea behind this was to provide each car with more than 1 radio to spread the risk of losing a node during operation.

The left side of the figure (with node DEU-MTR-5) shows the anchor towards the fixed network (located at an airfield tower in Greding). The next four nodes were realized within the DEU cars, the right four nodes were realized in NOR cars.

From this ideal configuration, two types had to be erased, as the availability was not given during the experimentation:

- The Harris radios (upper four ones in the figure) were used during one experiment with the Multi Topology routing but were not used for the other experiments due to the late entry into the experimentation
- The BGAN terminal could not be configured due to problems with the satellite service provider

Therefore, only 3 remaining radios (Flexnet, Kongsberg and HiMoNN) were available for the majority of the tests.

Each radio was available at the fixed network (tower) and in each national mobile segment at least in one entity.

At the beginning of the experimentation, separate radio tests were done, creating radio connectivity between four cars (each) and the tower, in the second phase, a combined convoy, based on both segments, was used.

Primary individual tests started using the ring road within WTD 81 (around the flight field), for convoy tests the route from Figure 4-9 was used.

The general node-configuration was done for the mobile nodes in the following way:

- On the wireless network side within the radios, a flavor of OLSR was running in some radios and the OSPF MDR protocol was running in the Kongsberg WM600 radios.
- To abstract from the real routing effects within the various radios, being used in a car, a full meshed internetwork layer was placed on top of the mobile nodes (including the fixed node DEU-MTR-5)
- On top of the full meshed tunnel, OSPF-MT was operated, to support Multi Topology Routing (MTR).
- Finally, on top of this black network, each node operated the pro-active IDP/TIBER implementation
- For multicast support, Simple Multicast Forwarding (SMF) was used within each mobile node (including node DEU-MTR-5)

4.2.1. MTR Field Experiment

During the CoNSIS field experiment we performed several tests to demonstrate the functionality of the MT-supported QoS architecture. Three MTR tests were specified for the field experiment:

- MTR-2: Demonstrate seamless mobility in a heterogeneous wireless network
- MTR-3: Test the use of multiple topologies for QoS purposes
- MTR-4: Limiting convoy network visibility for adjacent networks

The two weeks of experimentation were split into two parts. Most of the period was reserved for individual tightly directed tests, while the last few days were reserved for a common test. In this test, parts of the scenario were played out and selected functionality from the different tasks was demonstrated at the same time. All three MTR tests were conducted during the first test period and MTR-2 was also run during the scenario test. Here we report on the MTR-3 test and the MTR-2 test run during the scenario play. We refer the reader to [8] for results from all tests and details about the network and SW configuration. Figure 4-3 shows the radio networks deployed in the coalition convoy. Table 4-1 gives some information about the radio types.

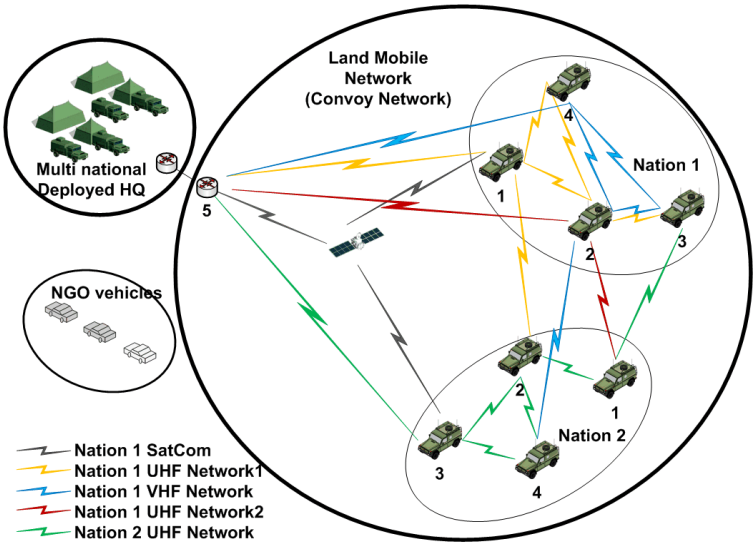

Figure 4-3: Land mobile network in CoNSIS (coalition convoy).

	Radio Type	Number of radios in the network	Shared channel data rate*
Nation 1 SatCom	Thrane &Thrane BGAN Ex. 727	3	384kb/s
Nation 1 UHF Network1	IABG, HiMoNN	6	1Mb/s - 11Mb/s
Nation 1 VHF Network	Harris , RF-7800S	5	64kb/s
Nation 1 UHF Network2	Rockwell Collins, FlexNet-Four	3	1Mb/s
Nation 2 UHF Network	Kongsberg, WM600	6	920kb/s - 2400kb/s

* The data rates are approximate values

Table 4-1: Radios used in the CoNSIS Convoy test network

For all three MTR tests we had planned to run the test with a more complex network connectivity situation, where more nodes and more radio networks had to be involved to provide a route from the source to the destination. Due to time constraints and problems with the availability of some of the radio networks, we completed the scaled down tests as presented below.

4.2.1.1. MTR-3: Test the use of multiple topologies for QoS purposes

In this test we wanted to show how topologies could be used to provide different paths for different traffic classes in a heterogeneous network. We also wanted to demonstrate how the topology concept could block traffic at the source for flows that could not be supported by the current network connectivity. We defined three different topologies for the CoNSIS field experiment in addition to the base topology. Table 4-2 show the association between topologies and radio types. For this test we also chose to configure the low data rate topology with the same interfaces and cost as the base topology. Thus the low data rate topology included all links.

Radio Type	Low data rate topology	High data rate topology	Low delay topology
Nation 1 SatCom	X	-	-
Nation 1 UHF Network1	X	X	X
Nation 1 VHF Network	X	-	X
Nation 1 UHF Network2	X	-*	X
Nation 2 UHF Network	X	X	X

* Originally these wideband radios were also intended to participate in the high data rate topology, but for testpurposes, as the SatCom network was not available for the field test, we chose to use this network as one of the networks that does not participate in all topologies.

Table 4-2: The use of the radio networks in the topologies

We initially planned to run this test for all topology types in the network. However, due to time constraints, we chose to run the test with traffic in the *low data rate* and *high data rate* topologies only.

The test starts with minimum route cost and full connectivity in both topologies. Traffic on both topologies is sent from NOR3 to all other NOR nodes (Figure 4-4). The traffic is marked in the IPv6 *traffic class* field with traffic classes that are associated with each of the two topologies (see Table 4-3 for the traffic classes associated with each topology). First NOR4 goes on a drive and eventually reaches a spot where there is no connectivity on the *high data rate topology* (see Figure 4-4, Test Phase). Figure 4-5 shows how traffic on the *high data rate topology* is blocked at this point, while traffic on the *low data rate topology* keeps flowing. The figure also shows the route changes (cost) for the route from NOR3 to NOR4 for the two topologies during the same timeframe. A route cost of 0 means that there is no route available in the topology table to the specified destination. The cost for the two topologies are the same as long as there is a route in the high data rate topology since the OSPF cost were set to prioritize high data rate links when these were available. The cost for the low data rate route increases much when a low data rate link is included in the path.

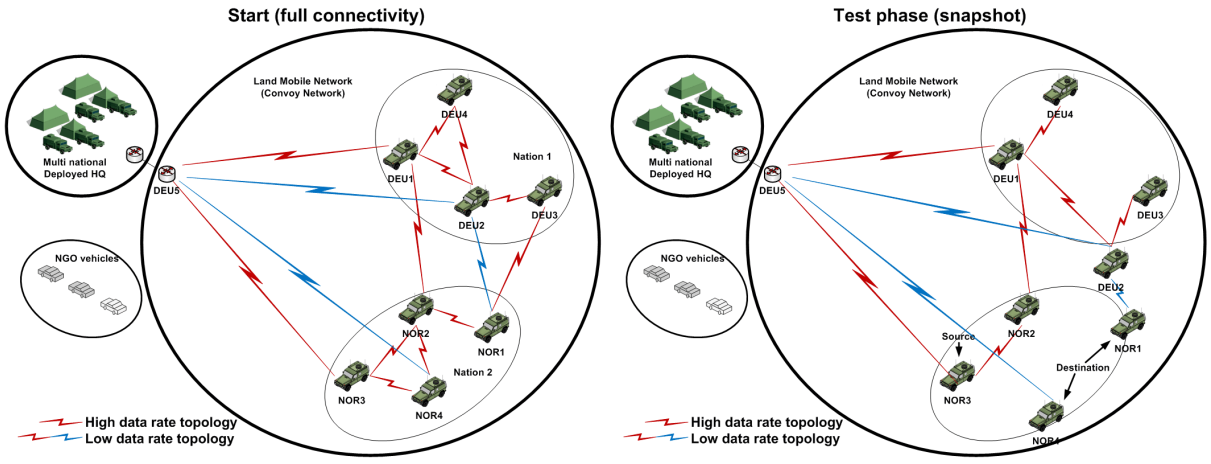

Figure 4-4: Network connectivity in two different segments

Figure 4-4 shows the network connectivity for two different topologies at the start of the test and at the test phase with bad connectivity for Nation1's UHF radio. All links (both red and blue) participate in the low data rate topology.

CoNSIS service	Low data rate topology	High data rate topology	Low delay topology
NFFI Service (AF21)	X	-	-
Chat application (AF22)	X	-	-
VoIP (MELPe 2400) (EF)	-	-	X
Image msg. service (AF11)	-	X	-

Table 4-3: Mapping between selected services (as given in Table 3-1) and the defined network topologies

Next NOR1 goes on a drive followed (a distance behind) by DEU2 in the same area. These vehicles also reach a spot where there is bad connectivity for the Nation 1's UHF radio. Figure 4-5 shows how traffic is again blocked on the *high data rate topology*, and the route cost on the route from NOR3 to NOR1.

The test clearly shows how traffic from traffic classes that cannot be supported end-to-end with the current network connectivity is blocked at the source instead of being sent into the network and dropped at the bottleneck link. This removes garbage traffic from the mobile networks, and thus allows the scarce capacity of these networks to be better utilized.

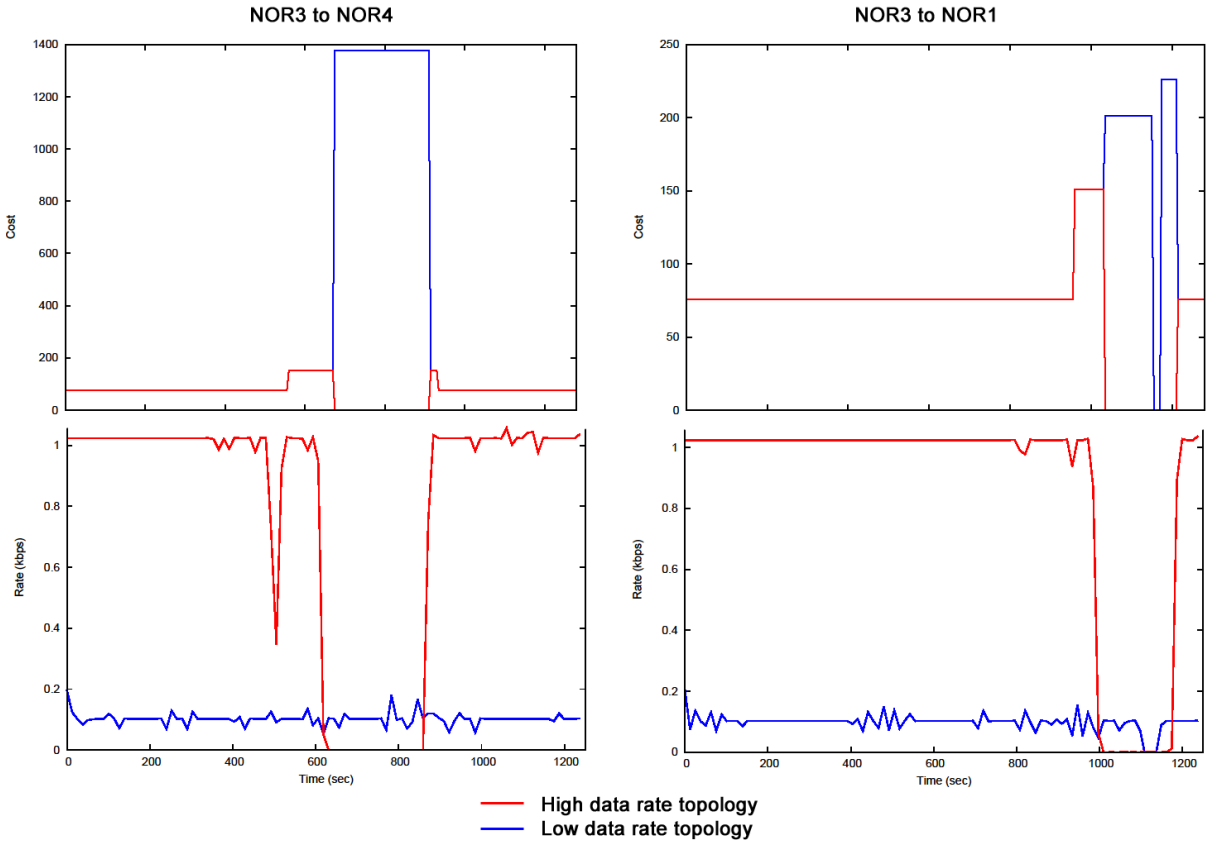

Figure 4-5: Cost diagrams

Figure 4-5 shows the cost of the path to the destination from the source, and the received traffic at the destination for traffic from NOR3 to NOR4 and NOR1.

Findings:

Multi Topology routing combined with DiffServ architecture realize the following benefits to a heterogeneous mobile network:

- Traffic tagged with different QoS classes can be routed on separate paths through the heterogeneous CoNSIS convoy network. This allows optimal choice of routing path

for a QoS type while at the same time preserving the robustness and resource efficiency present in a common heterogeneous transport network.

- Traffic associated with a traffic class that cannot be supported by the bottleneck link on the best network path, is blocked at the source (or at the edge of the network). This reduces the traffic load on the network.
- Normal DiffServ mechanisms for prioritizing, drop precedence and traffic shaping are configured on each network interface. This allows optimal utilization of the network resources in the different radio systems that are present in the convoy network
- The system supports a rerouting time of approximately 10s.

4.2.1.2. MTR-2: Demonstrate seamless mobility in a heterogeneous wireless network

The last days of the field experiment were reserved for a test common to all task groups, where parts of the CoNSIS scenario [5] were played. During this phase the MT-routing overlay provided the network service for traffic from the other tasks in the land mobile network. The MT-routing network represented the unprotected C-TNS (ref Figure 3-2) that covered the convoy. The traffic load on the convoy network from Task 2, "Information and Integration Services (SOA)" and Task 4, "Management" where encrypted by the security solutions provided by Task 3, "Security" prior to entering the convoy transport network. Due to the packet encryption, the network layer in the transport network could not do any packet inspection to deduct the traffic type of the packet to identify the require traffic class. In order for the network layer to provide a differentiated service for the network load, the data packet had to have a traffic class tag made available for inspection.

During the scenario plays we logged the routing tables periodically at all Norwegian nodes. We also sent some test traffic between the Norwegian nodes with low intrusiveness during the test.

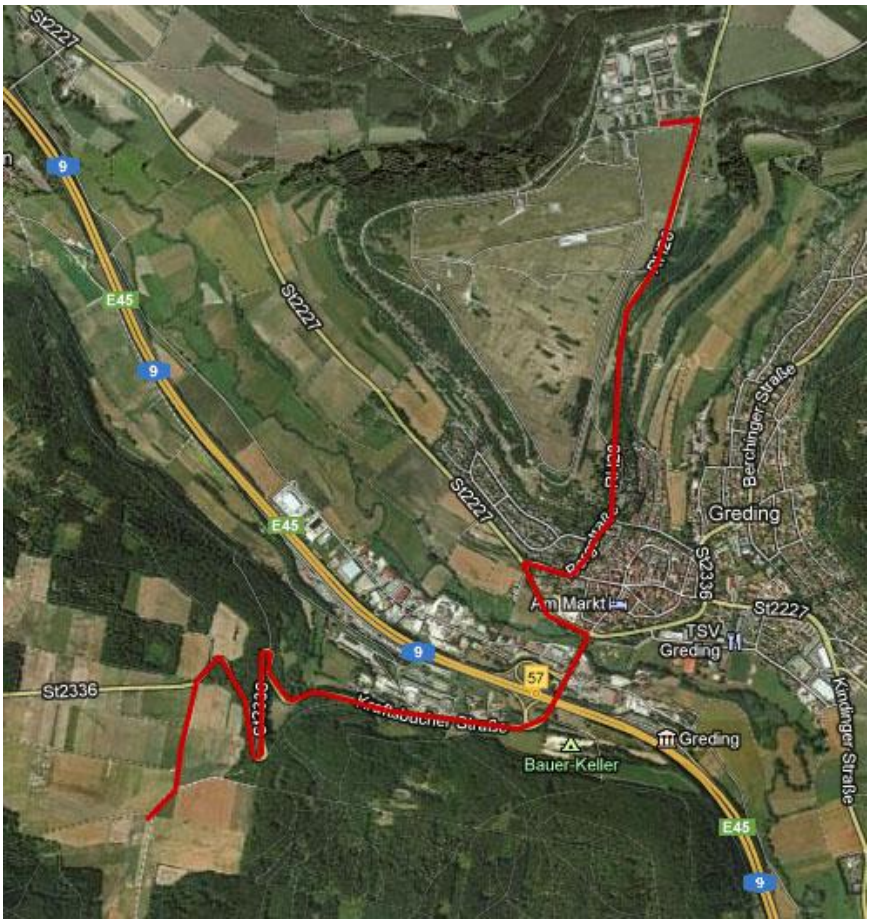

Figure 4-6: The scenario route for the convoy

The route that was used by the vehicles in the scenario plays is depicted in Figure 4-6. In the scenario the DEU (Nation 1) convoy part set off on the scenario route first. After a short time it lost network connection to the NOR (Nation 2) convoy part. This represents the phase 1a in Figure 4-7. Sometime later, the NOR convoy part set out on the same drive and eventually reached a spot where the networks of the two convoy parts merged (phase 1b in Figure 4-7).

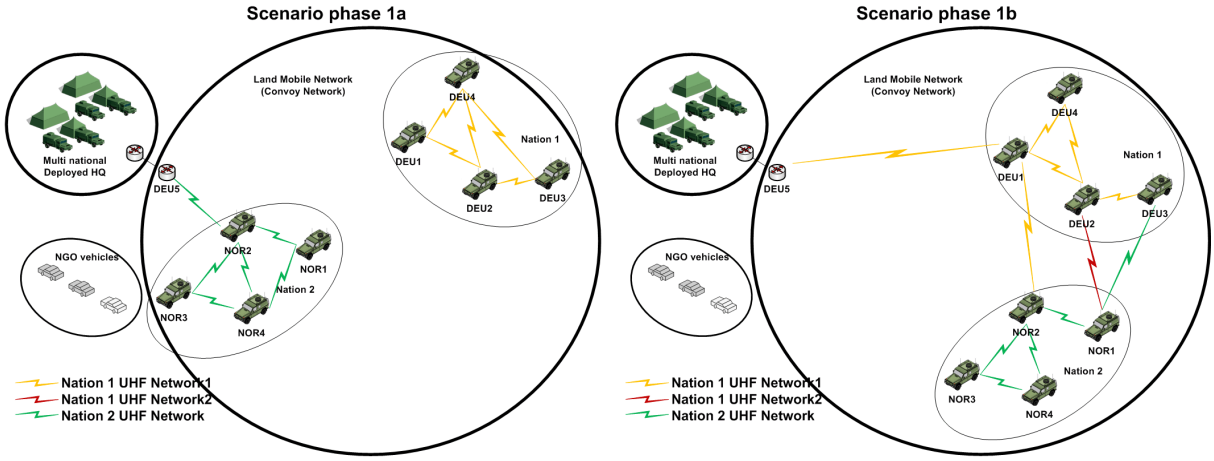

Figure 4-7: Convoy network connectivity during phase 1a and 1b of the scenario

Figure 4-8shows the cost of three routes between three of the NOR vehicles and three of the DEU vehicles and the cost between the same NOR vehicles and the deployed HQ (DEU5). NOR2 was equipped with the (DEU) *Nation 1 UHF network 1* and DEU3 was equipped with the (NOR) *Nation2 UHF network*. Thus when the convoy parts came within communication range of each other these routes should have a one-hop connection with the cost of the

OSPFv3 cost given to the specific radio type. Both of these radio types were also present at DEU5 in the deployed HQ. From the figure we see that most of the time when there is a route available, there is direct connection between the convoy parts. For short periods of time the cost doubles, which means that the route most likely goes via DEU5 in the airfield tower at WTD81. The antennas on this tower are elevated compared to the vehicle mounted antennas, thus the connectivity to the tower is better than the connectivity between vehicles in the hilly environment. NOR4 and DEU1 are not equipped with compatible radios, thus the cost of this route is always minimum one (DEU) *Nation 1 UHF network 1* hop and one (NOR) *Nation 2 UHF network* hop.

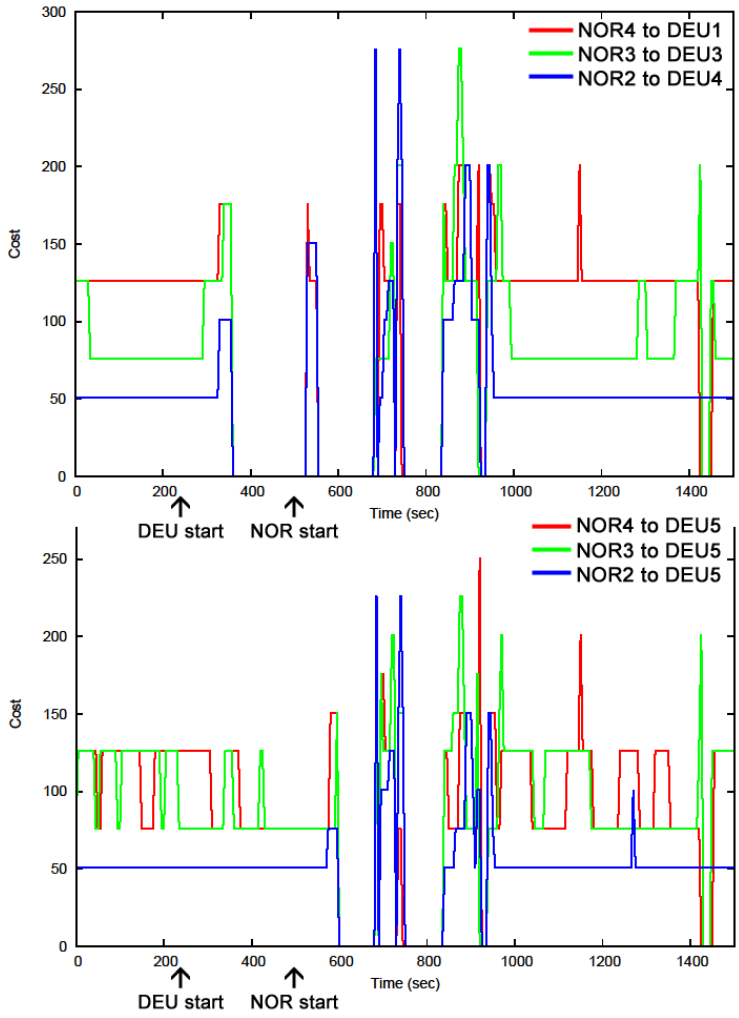

Figure 4-8: Route costs within the convoy

Figure 4-8 shows route costs between selected NOR vehicles and selected DEU vehicles and route cost between NOR vehicles and DEU5 (Deployed HQ). A cost of 0 means that there is no route

A rough description of the connectivity in the convoy during the scenario play based on the routing table cost and approximate start times given in Figure 4-8 goes as follows. The DEU convoy part starts driving at approximately 250s after test start. At time t=330s the path between the convoy segments is routed via DEU5 in the airfield tower. At time t=360s the DEU convoy segment loses all reach back connections. Approximately 500s after test start, the NOR convoy part start driving from the base. A short time after this there is a brief (50s) connection from the DEU convoy via the tower to the NOR convoy. At time t=600s the NOR convoy segment is also isolated without reach back connection. At time t=685s a direct connection between the two convoy segments is established over a bad radio channel. The NOR

convoy part has a reachback connection to the deployed HQ via the DEU segment. The convoy parts are again separated at time t=750. At time t=840s both convoy segments are reconnected via DEU5 at the tower, and at t=955s a direct radio connection between the convoys are established for the rest of the test period.

We see from the network cost figures that the MT-routing overlay is able to efficiently utilize all available radio networks in the convoy to connect all nodes in the convoy. From our log files we also see that it takes approximately 10s for the routing overlay to detect a lost link and reestablish a new route. This rerouting time was expected since we configured an OSPFv3 router *dead-interval* of 8s on the high data rate radio links.

However, we also see that there is a high frequency of route changes. This also means that the network is unstable and will show a high percentage of packet loss. We believe that two important reasons for the unstable network connections is the fact that the radios used are operating in the UHF frequency band, thus the channels are sensitive to obstacles (threes, buildings, etc.) between the source and the destination. The very high load on the network, and the fact that we were not able to prioritize routing messages on all interfaces (see [8] for more information about this problem), also lead to packet loss of routing messages, and thus erroneous selection of new routing paths.

Findings:

- The OSPF-MT overlay routing network efficiently connects all radio types in the CoNSIS convoy network. The result is a common heterogeneous mobile network
- The system supports a rerouting time of approximately 10s
- During the scenario tests most of the QoS mechanisms available in the MT-supported QoS architecture was not utilized. The consequence was that all traffic was treated as best effort traffic over most interfaces. At times the network load was fairly high and we network instabilities due to loss of routing packets.
- The overlay network as it was configured in the CoNSIS experiment does not scale to a large network. Other methods are available that can make the system more scalable

4.3. Experiment Analysis

4.3.1. Core Network Experiments

The network architecture being used at the deployed (or fixed) headquarter level is in principle stable. The results being generated during the Greding experimentation showed that most networks element being used are mature and efficient enough. The only restrictions being detected are those handling the aspect of a domain boundary between deployed and mobile network segments, esp. the QoS translation. Neither a fixed mode (as PIM-SM in the deployed part) nor a dynamic mode (as SMF in the mobile part) can be used vice versa. Here a specification lack was detected and theoretical and practical studies are necessary to solve this problem.

Findings:

The solving the multicast problem at the domain boundary between fixed and mobile networks was only possible to generate a local work around with static, fixed mappings between PIM-SM and SMF. This works for a proof of concept test, but is no stable solution.

Therefore a theoretical study and afterwards a practical testing is necessary to consider the behavior between those solutions being based on group membership management and protocols working without such a mechanism.

4.3.2. Experiments Regarding the Convoy

The initial tests during the Greding experimentation were executed at the beginning in two separated convoy segments. DEU and NOR started with homogeneous radios within the own segment, testing network coverage within the Greding area. These tests were done in the same region as the later combined tests, but limited to one radio, being installed in a subset of 4 cars and one radio being installed at the tower building within WTD 81.

These tests were executed in a way, that the convoy parts were leaving the WTD 81 area and then trying to get the maximum distance between cars, when running a convoy part both in hilly areas and inside a village.

As expected, the communication was broken between the cars and the tower, as soon as the radios were losing direct line connectivity (beyond a hill or between buildings in Greding).

The following figure shows the area of operation of the DEU cars:

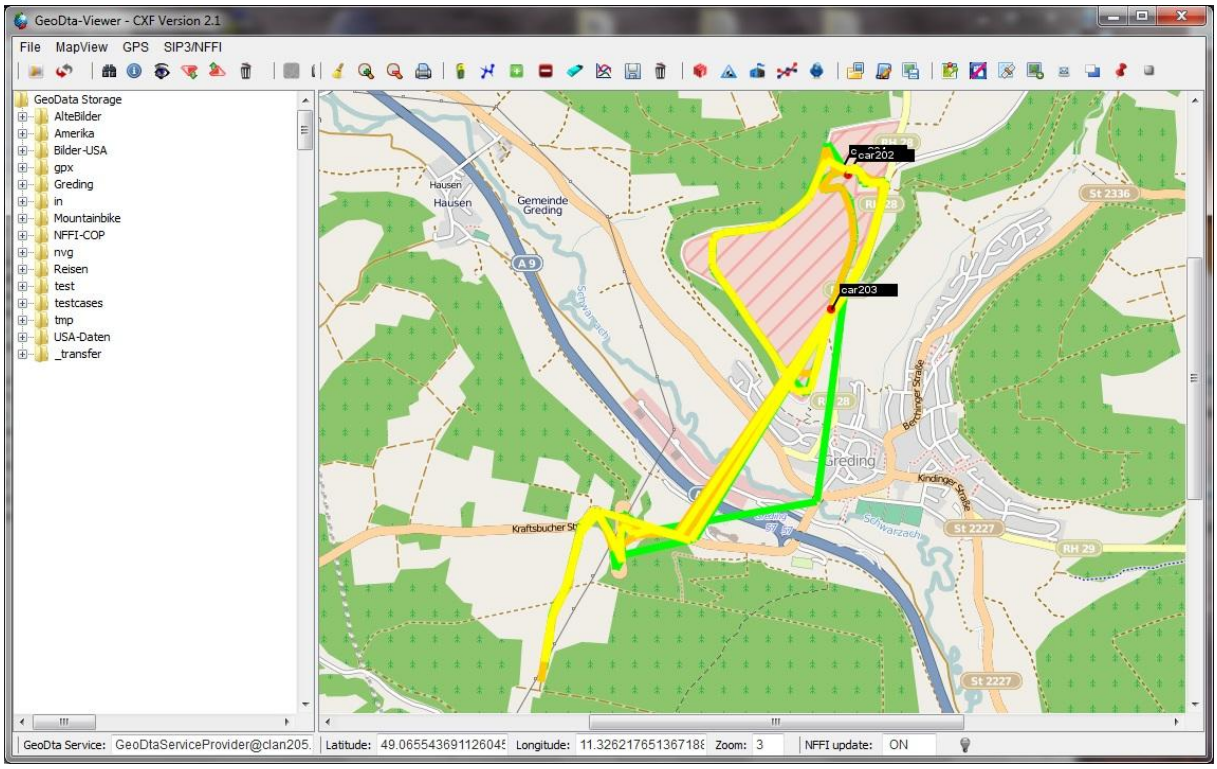

Figure 4-9: Principle area of operation of the DEU cars

The cars were using either the inside airfield of the WTD 81 (circle around the red-striped area) or were driving through Greding and the motorway A9 to the opposite hill south-west of Greding.

The connection was lost for a single car towards the tower both in the lower south-west part of the airfield (no direct line of sight) and outside the WTD81 up from the position of car203 up to the position 100m south-west of the motorway bridge on the opposite side of Greding (again, no line of sight). A single car was isolated from the network for a couple of kilometers both inside the WTD81 and in the topological depressed area of Greding. This result was expected because of the special topography in Greding, both for the DEU and the NOR radio types.

Findings:

The operation of a homogeneous DEU segment showed the expected results:

- The ad-hoc communication between all cars works well, the remote interconnection too, as long as line-of-sight radio connection was possible
- Any topological block worked immediately: As soon as there was no line-of-sight between two cars or between a car and the tower, the radio connection was interrupted; as soon as the reason for disruption disappeared, the radio connection was re-initiated immediately
- Applications using this radio connection were waiting, as soon as disruption was signaled, no buffer mechanisms were used at the network layer; this caused the behavior from Figure 4-9, that a node was jumping over a significant distance (jump between last possible and next possible radio connection).
- The WS-Discovery usage (from Task 2) had no hard consequence for the HiMoNN nodes, the traffic amount was moderate, messages in between during no radio connection were dropped and the exchange of new PDUs was restarted after network re-initialization
- Multicast traffic was not seen as a blocking factor, as the number of nodes was small and there was no significant traffic towards nodes without group members
- By definition, membership management was not necessary within a single mobile segment

A summary of the experiment Task1 did during the scenario phase of the Greding experimentation is described in chapter 4.2.1.2.

When interconnecting two national segments into a single one, either using one or two common radio sets, both unicast and multicast routing was initiated across technological boundaries immediate. Propagation of multicast packets was working well in both directions.

Experiment Analysis:

Based on the results being achieved in the Greding experimentation, the following areas should be considered for future R&D work:

- The multicast mechanisms being used are not compatible. Problems arising when using mechanisms with and without group membership management can be solved today only with a work around, as used in CoNSIS, but is not a global solution which means that networks using SMF cannot be used as transit networks
- Ad-hoc radio detection as used in CoNSIS is working sub-optimal: There should be a method to put a radio in sleep mode when it is isolated from the rest of the radios operating on the same waveform and frequency range.. In CoNSIS an isolated radio transmited Hello beacons permanently also when there was no answering system
- MTR was shown to work well in a controlled network environemnt in Greding. However due to limited use of the Harris VHF radio and lack of the Satcom service, there is still a need for testing in a more realistic network (e.g. with significant time delay).
- MTR currently build topologies based on static predefined link characteristics. The benefit of this is that this value is always a correct “typical value”. If there is no route to the destination in the chosen forwarding table, then it is certain that the traffic flow cannot be sustained. If there on the other hand is a route available, it is not certain that there is capacity on this route to sustain the traffic. In future work we want to investigate if dynamic parameters representing the real time resource situation for the links can be incorporated efficiently with the MT-routing protocol to better support the resource management mechanism.

4.3.3. Naval Task Force Experimentation

The CoNSIS Naval Task Force network architecture and testbed are outlined here. The test bed was located at the SPAWAR Systems Center in San Diego, California and connected to the convoy experiment via the Internet. Due to lack of an MOU the test bed was connected late to the experimentation network in Germany and there was little joint testing. National testing was performed with this topology shown below and the results are documented in a national test report.

The experimental network architecture consists of two Protected Cores (PCores), one designated for the national network and the other for the Coalition network. Each ship has point-to-point satellite links to a respective shore node corresponding to its PCore and is typically interlinked by line-of-sight (LOS) links that can be either using a Layer-2 bridge or a High Frequency (HF) radio using Layer-3 routing. The Figure below depicts the idealized overall network architecture. An "INE" is an In-line Network Encryptor. Landlines connect the US national shore station to that of a coalition nation. The shore stations have connections on the Plain Text (PT) side as well as via the PCore network.

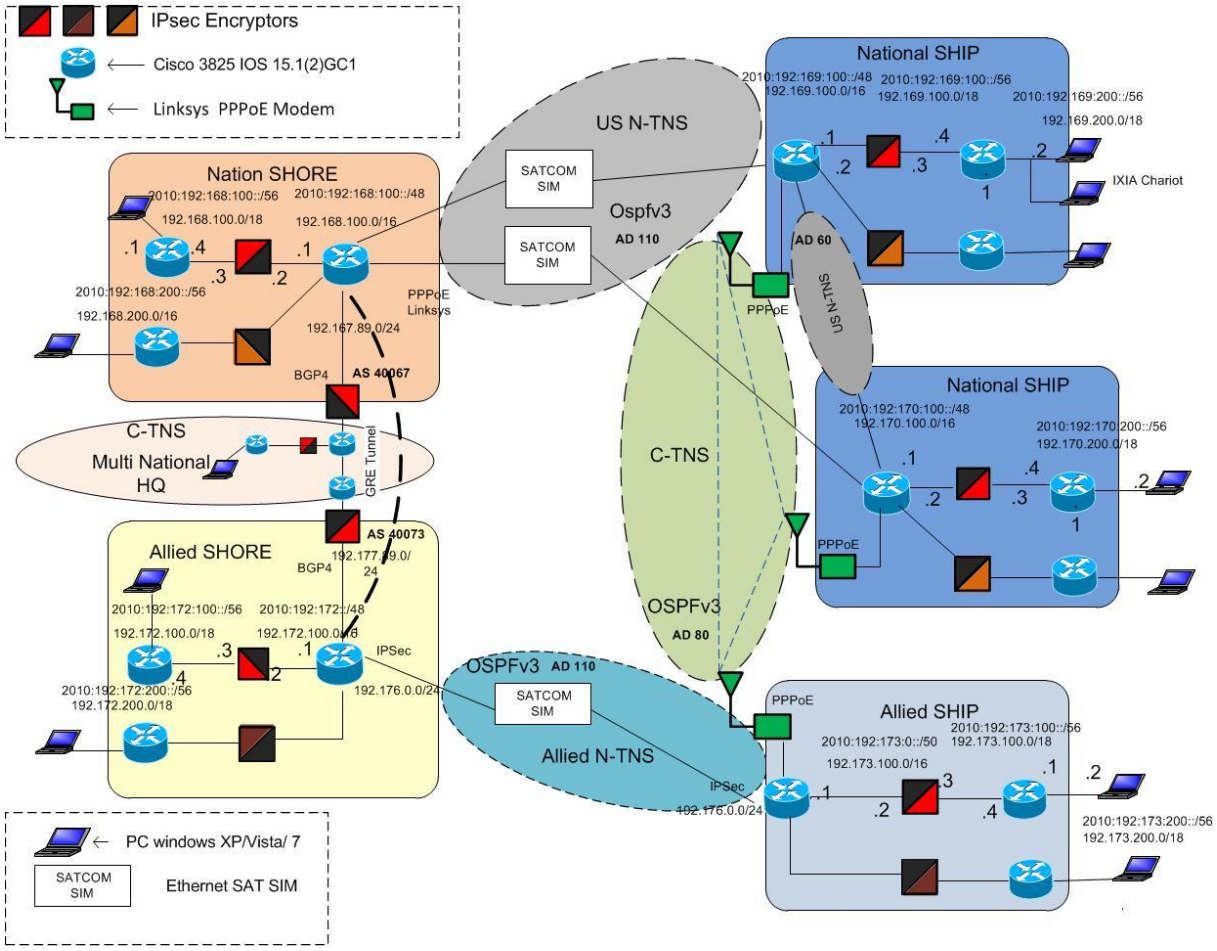

Figure 4-10: Simplified Naval Task Force Testbed Topology

An idealized testbed to demonstrate the Coalition Network Interface to support the Naval Task Force for the CoNSIS project is illustrated by the diagram in Figure 4-10. Two shore nodes and three ships are represented. Each of these ships has point-to-point satellite links to a shore node and is interlinked by a proxy that emulates a radio which supports PPPoE with Flow Credit and Link Metric extensions, and also makes the network connection appear to the router as a Layer-2 segment even if the radio is acting as a Layer-3 IP router. The IxChariot test tool is used to simulate applications, generate test traffic, collect traffic statistics, and produce data for graphic display and

visual presentation. Additionally, real applications (such as e-mail, chat, and FTP) have been installed for test purposes.
The key experiment objectives can be summarized as follows

- Demonstrate OSPFv3 with AF support can be used for mobile networks with reduced administrative overhead, i.e., IPv4 traffic can be routed via mobile interfaces with no need to be the same IPv4 subnets.
- Demonstrate QoS based on weighted fair queuing is possible on point-to-multipoint wireless connection using PPPoE with credit-based session flow control extension.
- Demonstrate improved network stability and control of routing path based on PPPoE with session-based link quality metric feedback extension.
- Demonstrate these features in an integrated testbed in relevant scenarios, described in the scenario testing section.

Objectives:

The test objectives are to demonstrate the following features in a testbed that realistically emulates the tactical network of a Naval Task Force.

- Demonstrate that PPPoE protocol with link metric extension can control the forwarding path based on link quality feedback.
- Demonstrate OSPFv3 with AF support can be used for mobile networks with reduced administrative overhead. That is, to demonstrate that IPv4 traffic can be routed via mobile interfaces that have no need to be same IPv4 subnets.
- Demonstrate QoS based on weighted fair queuing is possible on a point-to-multipoint wireless connection using PPPoE with traffic flow credit extensions.
- Demonstrate improved network stability and control of routing path based on use of PPPoE with link metric extensions
- Demonstrate use of all these features in an integrated test bed using several realistic scenarios.

In short, the test goals are to demonstrate a network that does not require pre-planned addresses on the mobile networks, rapid network convergence, effective dynamic routing multicasting of data between nodes. These demonstrations were performed in a testbed setup designed to emulate the conditions expected in a tactical naval network.

Auto configuration - The mobile network interfaces were enabled to auto configure with IPv6 link-local addresses. This allows mobile nodes to join and start communicating with other enclaves in the network without the need to have pre-planned addresses, thus reducing administrative burden. The link-local address is derived from the Ethernet MAC address. Cisco implementation requires an IPv4 address to be configured on the mobile interface, even though it is not used for routing and does not need to be configured in the same subnet as other mobile interface in the ad hoc network. It was verified that the OSPFv3 processes discovered each other via the link-local addresses, formed neighbors, exchanged routing databases and forwarded traffic as expected.

IPv6 Address Family Support - OSPFv3 uses IPv6 for router information exchanges and packet forwarding. Since users still need to use IPv4 for some time in the future, Cisco implementation of OSPFv3 with AF support other than IPv6 unicast AF allows OSPFv3 to forward IPv4 traffic, thus facilitating interoperability within realistic mixed IPv4 and IPv6 network environment. This Cisco implementation of AF support was tested. IPv4 connectivity across the IPv6 backbone was verified.

Mobile Network Convergence - PPPoE with extensions for Credit Flow and Link Metrics allows faster network convergence. Test results show a faster response to mobile units entering and exiting an ad hoc mobile network. In addition, network traffic is more quickly re-routed when a link is marked down. The convergence time depends on the software configuration, but for this Cisco implementation node the network convergence time for a node entering or leaving the mobile networks was observed to be near real-time, about 5-6 seconds, compared to 40 seconds for the dead time of the standard OSPF configuration.

Re-routing based on Link Quality Metrics - This test session demonstrates the ability to re-route traffic based on the changing quality of the links. In this test, the OSPFv3 dynamic routing cost of Cisco routers is based on the link metric values, such as Max-Data-Rate (MDR), Current-Data-Rate (CRD), Latency, Resources and Relative Link Quality (RLQ) of radio link characteristic fed back to the routers. These metrics are defined in [4] in terms of a type-length-value (TLV) message which is used to report the link quality parameters. In a network of three mobile nodes the link metric RLQ (a non-dimensional number from 0 to 100 inclusively, representing the relative link quality with a value of 100 represents a link of the highest quality [4]) was manually changed on the preferred link and it was observed that traffic was re-routed

QoS via PPPoE with extensions - This Quality of Service test demonstrates that Class Based Weighted Fair Queuing (CBWFQ) works on virtual interfaces via a point-to-multipoint link using PPPoE with extensions for credit flow and link metrics. A QoS policy, if configured, limits the bandwidth allowed on a virtual link and prioritizes the flows of several different types of traffic. When the allowed bandwidth is reduced, it is observed that the traffic flows are impacted according to the configured QoS policy configured on the Cisco Virtual Multipoint Interface (VMI). In this test, IxChariot and/or installed applications are used to generate traffic, including video, FTP, Critial FTP, and web (TCP) traffic.

Routing Issues -During the course of network design and initial testing, several routing issues surfaced. Primary among them are the following three issues, namely (1) manual configuration of Border Gateway Protocol (BGP), (2) duplication of OSPF's Link State Advertisements (LSAs), and (3) "sticking" BGP routes. First, the routing domains between nations have to be separated to prevent routing loops. This is normally done with BGP, but BGP is manually configured and this is not practical in the tactical environment. For this reason redistribution of routes between OSPF processes was used to automatically advertise routes, which is a proprietary feature available on Cisco routers.

Secondly, when routes are redistributed between OSPF processes, increased the overhead on the routing protocol on the network. This may be resolved by OSPF filtering and will be investigated in the future.

Finally, BGP was used on the shore between US and allied shore stations. There has been an issue with the routes "sticking" when the ship/shore links cycle up and down. This was resolved with by the use of a "non-exist" statement on the shore router.

Scenario testing - The six (6) scenarios were tested as the following:

- Basic scenario - Two Network Operations Centers (NOCs), three satellite links three ships with LOS links
- Re-routing of traffic via coalition partner when satellite communications (SATCOM) link goes down
- Link restoral SATCOM to shore
- One SATCOM link – LOS relay between ships.
- No SATCOM – only LOS routing between ships

- Plain-Text routing between US shore and allied shore

Naval Task Force Summary:

Throughout phases of this ongoing effort we have been gathering lessons learned and observing and tracking emerging trends and technologies relevant to designing a Naval Task Force that enables secure delivery of network-based applications and services over radio links to support information sharing.

While IP Network architects would like to the radio link to be a transparent network segment, which operates at the Open Systems Interconnection (OSI) Layer 2, radio manufacturers often design the radio as a router, with the connection made at OSI Layer 3. The extended PPPoE protocol is a step in the right direction, which has been promoted by radio and router manufacturers. This plausible intermediate step is not without issues – in particular, multicast not being supported in an efficient manner. Currently, multicast is converted to unicast and forwarded via virtual PPP connections set up by the PPPoE protocol.

Protocols in development such as the Dynamic Link Exchange Protocol (DLEP) may handle multicast as well as applications and services such as full-motion video and video-teleconferencing more efficiently. As such, new protocols will be investigated in future work.

It is noted that there is at least one radio that supports these PPPoE extensions; however, its cost is prohibitive for use within the current budget of this project. Future testing will involve commercial radios and sea trials.

5. CONCLUSIONS AND FUTURE WORK

Task 1 has studied, implemented and tested several mechanisms to provide end-to-end connectivity and QoS within the communications constraints and dynamic topology imposed by highly mobile tactical networks and their deployed backbone. Major results are:

- Definition of a technical profile to describe real-time QoS parameters of a black transport network (Administrative System) and the QoS capabilities of the system. The technical profiles of an end-to-end path are collected and the values in the different technical profiles are aggregated to describe the QoS available on the end-to-end path. The end system can use the aggregated Technical profile data to adapt the data to suite the available network QoS.
- Establishment of an overlay to interconnect the mobile ad hoc networks (MANET) created by incompatible military radios. The result is a common black heterogeneous MANET transport network that covers all available radio networks in a coalition operation.
- Multi Topology (MT) routing to build topologies that represent different QoS characteristics of the heterogeneous MANET (e.g., high data-rate, low delay). Associate traffic classes to the topologies to provide some differentiated services in the heterogeneous MANET and aid a network resource management and admission control element.
- A study of the applicability of PPPoE and its extension defined in RFC5578 for radio to router communication in order to enhance QoS and resource management in heterogeneous military MANET.
- A solution for integration of Tactical Data Link messages in services running on IP networks. A gateway solution advertising the TDL messages as a service in the service infrastructure was chosen.
- A “proof of concept” solution for end-to-end multicast over the traditional multicast protocol PIM-SM and the flooding based SMF protocol.

Based on the results from the theoretical considerations and the practical results achieved during the Greding experimentation, the following activities are recommended in further CoNSIS phases:

- Theoretical specification and practical testing of seamless multicast communication between domain with and without membership management
- Transparent generation and automatic report of QoS parameters at Link Layer and consumption at Network Layer
- Integration of operational considerations into policy-based routing
- Optimization of Cross-Layer communication technologies
- Integration of sensor and effector networks into the CoNSIS network architecture

6. REFERENCES

[1] NATO Network Enabled Capability Feasibility Study Executive Summary v. 2.0, October 2005.

[2] G. Hallingstad and S. Oudkerk, “Protected core networking: an architectural approach to secure and flexible communications”, Communications Magazine, IEEE, 2008, 46, pp. 35 -41

[3] M. Hauge, M.A. Brose, J. Sander, and J. Andersson, "Multi-topology routing for improved network resource utilization in mobile tactical networks," *MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010* , vol., no., pp. 2223-2228, Oct. 31 2010-Nov. 3 2010.

[4] M. Hauge, CoNSIS Task 1, “QoS-classes for the CoNSIS test and demonstration architecture”.

[5] “System and Experimentation Architectures - Version 1.0”, CoNSIS/Task 5/DL/002, September 2011

[6] CoNSIS/Task5/DL/001 System and Test & Demonstration Architectures (Draft 0.3), 26. March 2010.

[7] R. M. van Selm, G. Szabo, R. van Engelshoven, and R. Goode, *Ip QoS standardisation fo the NII*, RD-2933, NC3A,(Nato Unclassified), Apr. 2010.

[8] M. Hauge et al., “*Multi-Topology Routing – QoS functionality and results from field experiment*”, CoNSIS/Task1/DU/003, Nov. 2012.

[9] S. Mirtorabi and A. Roy, "Multi-topology routing in OSPFv3 (MT-OSPFv3)." *draft-ietf-ospf-mt-ospfv3-03.txt* (work in progress), July 2007

[10] P. Psenak, S. Mirtorabi, A. Roy, L. Nguyen, and P. Pillay-Esnault, "Multi-topology (MT) routing in OSPF." *RFC 4915*, June 2007

[11] S. Blake et al., "An architecture for differentiated serv." *RFC2475*, 1998

[12] D. Grossman, "New terminology and clarifications for diffserv." *RFC 3260*, 2002

[13] R. Ogier and P. Spagnolo, "Mobile ad hoc network (MANET) extension of OSPF using CDS flooding." *RFC 5614*, Aug. 2009

[14] Vyatta, http://www.vyatta.com

[15] Quagga Routing Suite, http://www.quagga.net

[16] OSPFv3 MANET MDR, Boeing, http://cs.itd.nrl.navy.mil/work/ospf-manet/

[17] CoNSIS/Task5/DL/001 System and Test & Demonstration Architectures (Draft 0.3), 26. March 2010.

[18] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol." *RFC 3626*, 2003.

[19] B. Berry, S. Ratliff, E. Paradise, T. Kaiser, and M. Adams, “PPP Over Ethernet (PPPoE) Extensions for Credit Flow and Link Metrics,” *RFC 5578*, Feb. 2010

[20] S. Ratliff, B. Berry, G. Harrison, S. Jury, and D. Satterwhite, “Dynamic Link Exchange Protocol (DLEP),” *draft-ietf-manet-dlep-03.txt* (work in progress), Aug. 2012

[21] D. Dubois, A. Kovummal, B. Petry, and B. Berry, “Radio-Router Control Protocol (R2CP),” *draft-dubois-r2cp-00* (work in progress), March 2011

[22] L. Landmark, K. Øvsthus, and O. Kure, "Routing trade-offs in sparse and mobile heterogeneous multi-radio ad hoc networks,", *in proceedings MILCOM* , pp. 2229-2236, San Jose, CA, USA, 31 October 2010

[23] Simon, P.: Technical Profile – Definition and Associated Processes,CG/UM-ESIO/IDRE/10.099/V1.1, July 27, 2010

[24] Simon, P.: Technical Profile and Communication Chains, CG/UM-ESIO/IDRE/10.100/V1.1, July 27, 2010

[25] Simon, P.: Technical Profile and User Services, CG/UM-ESIO/IDRE/10.101/V1.1, July 27, 2010

[26] Simon, P.: End-to-End QoS – Relationships between QoS, Technical Profile and User Profile, CG/UM-ESIO/IDRE/10.096/V1.1, July 27, 2010

[27] Simon, P.: End-to-End QoS – Differentiated QoS in Network of Different Operational Levels, CG/UM-ESIO/IDRE/10.098/V1.1, July 27, 2010

[28] Bret, N., Ridard, B., Simon, P.: Technical Profiles – Lessons Learnt from Demonstration Tests, CG/UM-ESIO/IDRE/11.236/V1.0, dated November 4, 2011

[29] Bret, N., Ridard, B., Simon, P.: End-to-End QoS – Lessons Learnt from Demonstration Tests, CG/UM-ESIO/IDRE/11.237/V1.0, November 4, 2011

[30] List, M.: PPPoE (RFC 5578) Implementation, Sept. 8, 2010, CoNSIS/DEU/Task1/DU/001

[31] Macker, J.: Simplified Multicast Forwarding, March 6, 2012, IETF, draft-ietf-manet-smf-14

[32] Umlauf, R.: SCIP-Enabled-Gateway, v.1, Sept. 8, 2010, CoNSIS/DEU/Task1/DL/002

[33] Umlauf, R.: Reliable UDP, CoNSIS/DEU/Task1/DU/002

[34] List, M., Seifert, H.: QoS-Manet-Considerations, Dec. 01, 2009, CoNSIS/DEU/Task1/DU/003

[35] Umlauf, R.: MLP-Services, Sept. 2, 2011, CoNSIS/DEU/Task1/DU/004

[36] Fey, M., List, M., Seifert, H.:Net Framework, May 2008 30, CoNSIS/DEU/Task1/DU/005

[37] Hauge, M.: CoNSIS QoS-classes, v0.2, Feb. 6, 2012, CoNSIS/NOR/Task1/DU/001

[38] C. Bow-Nan, J. Wheeler, and L. Veytser, "Radio-to-router interface technology and its applicability on the tactical edge." Communications Magazine, IEEE, vol. 50, no. 10. pp.70-77, October 2012

[39] Tran, T.: Proactive Multicast-based IPsec Discovery Protocol Description & Specification, INSC II/Task 2/US/003

7. ABBREVIATIONS

AF	Assured Forwarding
AS	Autonomous System
BE	Best Effort
BGP	Border Gateway Protocol
CE	Colored Enclave
CoS	Class of Service
C-TNS	Coalition Transport Network Segment
DL	Data Link
DNS	Domain Name System
DSCP	DiffServ Code Point
ECN	Explicit Congestion Notification
EF:	Expedited Forwarding
EGP	Exterior Gateway Protocol
FEC	Forward Error Correction
FTP	File Transfer Protocol
GRE	Generic Router Encapsulation
HF	High Frequency
HQ	headquarter
HTB	Hierarchical Token Bucket
HTML	Hyper Text Mark-up Language
HTTP	Hyper Text Transfer Protocol
ICE	Inner CE
IGP	Interior Gateway Protocol
IP	Internet Protocol
LAN	Local area network
LDAP	Lightweight Directory Access Protocol
LD-TLV	Link Description - TLV
LFN	Long and Fat Network
LSA	Link state advertisement
MANET	Mobile Ad Hoc Network
MDR	MANET Designated Router
MLPP	Multi-level precedence and priority
MoU	Memorandum of Understanding

MPL	Military Precedence Level
MPLS	Multi Protocol Label Switching
MT	Multi Topology
NCIA	NATO Communications and Information Agency
NFFI	NATO Friendly Force Information
NII	Network and Information Infrastructure
N-TNS	National TNS
OLSR	Optimized Link State Routing
OSPFv3	Open Shortest Path Firstv3 (for IPv6)
OSPFv3-MT	Open Shortest Path Firstv3 – Multi-Topology
PCN	Protected Core Networking
PHY	Physical Layer
PRIO	Priority Queue
QoS	Quality of Service
RMT-sTLV	Router Multi-Topology sub-TLV
RSVP	resource ReSerVation Protocol
SA-data	Situational Awareness data
SBC	Service Based Class
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SPF	Shortest Path First
ST	Single Topology
SW	Software
TFC	Traffic Flow Confidentiality
TE	Traffic Engineering
TLV	Type-Length-Value
TNS	Transport Network Segment
TOS	Type of Service
UHF	Ultra High Frequency
VHF	Very High Frequency
XML	eXtended Markup Language