



Danish Defence Research Establishment

DDRE REPORT NO. M-19/2005

DDRE Report

The Target Architecture for the ICT Systems in the Danish Defence

WP₃

Defence Communication (DEFCOMM)

BY
Gert Hvedstrup Jensen
Alfred Møller
Lars Brandt
Jens Stavnstrup
Hans Henrik Schultz
Hans Marqvardsen

DEFCOMM

The Target Architecture for the ICT Systems in the Danish Defence

WP3

Defence Communication (DEFCOMM)

by

**Gert Hvedstrup Jensen
Alfred Møller
Lars Brandt
Jens Stavnstrup
Hans Henrik Schultz
Hans Marqvardsen**

Abstract

This report is intended to serve as a steering point for the development of Information and Communication Technology (ICT) Systems in the Danish Armed Forces. The evolutionary development of these systems for the next 10-15 years will be strongly influenced by the rapid advances in technology and by the principles of network based operations (NBO). Other guiding principles are the use of commercial off the shelf products (COTS) wherever possible and as loose a coupling between systems as possible.

The target architecture is a concatenation of different views, encompassing basic principles, a reference model and technology views: IP-convergence, Service orientation, Local-, regional-, global communications, Evolutionary development, Organisational considerations, End-to-end communications, Addressing and routing, Quality of service, Network management, Interoperability and Security. The overall result of this is the all-IP target architecture with applications that collaborate in a Service Oriented Architecture (SOA).

To meet requirements on robustness, security and jamming resistance the communication will be based on many different transmission means such as the civilian telecommunications infrastructure, SATCOM, dedicated military links (e.g. link 16) and combat net radios and cellular radio systems. The software defined radio technology will be a future vehicle for obtaining multi-role and multi-frequency capabilities in one package.

Non-IP subsystems, eg military tactical data links such as Link 16, will be in existence for decades and is anticipated to connect to the global IP network through gateways.

The greater part of the target architecture is based on known and mature technology, and it will be a direct basis for the more detailed system architecture and subsequent acquisitions of ICT systems. A part of the target architecture is based on a conservative prediction of the technological development. The realization of these few parts must wait for the emergence and maturation of the technologies.

Requirements to interoperability flexibility and adaptability at the application level are met by adhering to a SOA. This permits a loose coupling between the component applications which has a number of advantages including robustness, the ability to integrate components to new applications as needed is met, and the ability to have components evolve at their own pace.

The target architecture will evolve through a number of stages. In this report we consider a time span of 15 years from now, where the architecture goes through 2 major stages towards an all-IP network as a basis for SOA mainly implemented as Web Services.

Summary

This report is the third and final work package of the DEFCOMM work and describes the target architecture for the *Information and Communications Technology (ICT) Systems* in the Danish Armed Forces. The results are based on the first two reports of the DEFCOMM work, which consist of analysis of selected scenarios and the requirements on information *in network based operations (NBO)*. These three reports should be regarded as a unified whole.

The DEFCOMM work will support the transformation in which the Danish Defence is heavily engaged. The transformation involves in the technological arena a transition from the platform centric operations towards NBO. Another important trend is the fusion of administrative and operational systems, and the desire to be able to share information not only within the military area, but across ministerial boundaries and with suppliers and even private citizens. One prerequisite for this increased network centrality is the establishment of a networked information infrastructure.

The DEFCOMM work is done at the Danish Defence Research Establishment (DDRE) in close co-operation with HQ Chief of Defence CCIS Staff (IS2), and the Royal Danish Defence College.

The target architecture is an overall coarse grained structural design that describes a future, ie10-15 years, system of systems. It identifies the main components and the relations between these components in the overall ICT systems infrastructure. This work forms a gradual transition towards a more detailed *system architecture*. The level of detail is chosen so that the target architecture will be relatively independent of technological details, so a certain degree of durability can be assured.

As a basis for the target architecture, a reference model is developed. This conceptual model is a layered model, consisting of a *service or application layer*, an *integration layer*, a *convergence layer*, and a *transmission layer*. The convergence layer is the part of the communication that homogenizes the system in the sense, that by using the Internet Protocol (IPv6 or IPv4), it is possible to create a network of networks that in principle allows all ICT systems to be connected. At the service and integration layers, SOA will be the homogenizing factor. SOA allows a loose coupling between the systems, but allows a flexible and robust method for integration and formation of applications.

To meet requirements on robustness, cost, security including jamming resistance, the communication will be based on many different transmission means such as the civilian telecommunications infrastructure, SATCOM, dedicated military links (eg Link 16) and combat net radios, and cellular radio systems. The software defined radio technology will be a vehicle for obtaining multi-role and multi-frequency capabilities in one package.

The target architecture will evolve through a number of stages. In this report we consider a time span of 15 years from now, where the architecture goes through two major stages towards an all-IP network as a basis for SOA, in the short term, mainly implemented as *Web Services*. Non-IP subsystems, eg military tactical data links such as Link 16, will be in existence for decades and is anticipated to connect to the global IP-network through gateways.

The evolution of the application part of the architecture and the communication part are considered separately, although the application architecture is critically depending on the communication architecture. The development towards the target architecture may be divided into three stages, approximately covering five years each.

The first stage, covering the period from now (2005) until the year 2010, will be characterised by the following items:

- Standards for service descriptions and service brokers must be selected.
- Methods for acquisition, development, and managing services must be developed.
- All new applications with functionality or data that are to be distributed will have as an option to be service oriented at the end of the period. The possibility of service-orientation will be a requirement on all new ICT acquisitions, and there must be a waiver if they can not be implemented in an SOA. They will have the option to be implemented as web services.
- A few legacy applications should be wrapped so that they can meaningfully be shared as web services. Candidates are parts of the CCIS of the three services and parts of DEMARS. These applications may serve as demonstrators, and thus pave the way for further successes.
- The rules and principles of the military SOA are established. Applications that follow these rules are *net worthy (net ready)*. The rules must be in accordance with the rules of anticipated coalition partners.

In the next stage, the period 2010- 2015 the feasibility and added value of SOA has been demonstrated. This stage is therefore characterised by:

- All new applications with functionality or data that are to be distributed will be service oriented, in the sense that they follow the rules that allow them to be part of the defence SOA. The possibility of service orientation will be a requirement on all new ICT acquisitions except for the dedicated or real time systems, and there must be a waiver if they can not be implemented in a SOA. *Web services* are the most likely platform.
- Old systems will be wrapped in the sense that they will be given interfaces that allow them to be part of the military SOA.

The final stage, reached approximately in 2020 presupposes a further technological development allowing more systems, including real time systems to be implemented as SOA. At this stage, security problems, management of these systems of systems and human computer interaction problems have hopefully been solved. This means that almost all shareable resources are accessed as services. It is not obvious that *web services* in its present incarnation will be the preferred vehicle at this stage!

The evolution of the communications part of the target architecture is parallel to the application architecture. Basically it will evolve through three main stages, from the present situation towards an all-IP network. The baseline may be characterised as:

- Many heterogeneous systems with their own standards and protocols. No network of networks is present, but many networks are based on the IP-suite. No common directory structure and name space. Little support for NBO.
- The CCIS of the three services are different, but may communicate by use of standardised messages and dedicated transmission channels.
- The dedicated tactical data links (eg link 11 and link 16) can not immediately be integrated into the IP-network.

In the present stage, some integration and some experimentation with the formation of networks of networks are possible. In the timeframe of 5 years, the formation of an embryonic network of networks is possible, and major systems such as DACCIS, NECCCIS, and RDNCCIS will be able to communicate via IP-network and provide some services to each other. At this stage rules and evaluation criteria for *net worthiness* must be defined.

In the midway stage, an increasing number of networks are either IP based, or coupled to the larger network of networks through gateways. This means that the overall network may be used as a communication mean between the dedicated systems. Gateways in pairs are no longer necessary. Both the major part of operational systems and administrative systems are connected to the overall *network*. This stage is prepared for NBO, and large scale experiments and exercises are possible. The network of networks will comprise an increasing number of systems, and new systems will have the IP as the native network protocol. The midway stage is feasible within a timeframe of 10 years.

In the final stage- which may be a vision- all networks are IP-based. All communication entities have an IP-address, and management of the *network* itself and most components may be performed over the network. The *network* fully supports NBO, and it is compatible with the networks of coalition partners and NATO. Gateways are no longer necessary for transmission purposes.

The greater part of the target architecture is based on known and mature technology, and it will be a direct basis for the more detailed system architecture and subsequent acquisitions of ICT systems. A small part of the target architecture is based on a conservative prediction of the technological development. The realization of these few parts must wait for the emergence and maturation of the technologies.

From a technical point of view it is possible to integrate most of the military and total defence networks into a network of networks by use of the IP-suite. The IP-suite will allow a convergence of all relevant networks. Further, convergence at the application level can be achieved by use of an SOA.

The proposed target architecture including all the presented architectural views should be used as guidance for planning, acquisition, and maintenance process for ICT. This includes the development of system architectures – a detailed instantiation of the target architecture with available technology and standards.

The ICT aspects must be assessed for all NBO related acquisition, including all sensors and effectors.

It is recommended to use a staged approach, where a number of well defined milestones, manages the development into an overall network of networks. The goal will be to integrate as many networks as possible into the overall scheme, and to have as many (all) networks as possible to use the IP as the native network protocol. Many networks already use the IP, but it will be necessary to use gateways to connect some of the networks to the global network. The first stage could be development of an IP-based backbone as basis for a flexible and dynamic infrastructure.

This means that in all cases, the acquisition process must include an assessment of the IP-capabilities of the communication equipment, including effectiveness of IP-interfaces and aspects of Quality of Service (QoS), security, management, etc.

Groups of networks such as administrative and operational networks may at least for some time have to be separated by information flow devices for security reasons. To limit damage from failure or intrusion incidents the total network must be segmented, logically or physically.

To fully exploit the network of networks, a global and integrated directory service for the total network of networks should be available.

Apply unified network management wherever possible. This will require that a management standard should be defined, and that all relevant networks and network components must follow the standard.

The proposed architectural guidelines are in accordance with the anticipated coalition partners, and should remain so. NATO and other international studies such as NNEC Feasibility Study, TACOM Post 2000, and MIP are examples of current studies to follow.

To obtain flexibility and loose coupling between component systems, it is recommended to use SOA as the overall architectural principle.

It is strongly recommended to exploit the principle of loose coupling to let the different systems (services and service consumers) evolve at their own pace. This includes tactical networks and other dedicated networks.

Make adherence to the general principles mandatory. Stove-piped systems should cease to exist. Legacy systems may be integrated by wrapping.

Conduct experiments to demonstrate the use, the advantages, and technological feasibility of the principles. This may involve Danish or other relevant industry in partnering ventures to conduct Concept Development and Experimentation (CDE). It is strongly recommended that COTS technology should not be implemented before it has reached a mature state.

Work towards semantic interoperability by using a common joint data model such as JC3IEDM, and ontologies.

Develop measures based on simple metrics to evaluate the degree of network readiness of all relevant present and future systems and components. Use the methods in the acquisition process.

It must be emphasised that the recommendations above are not without a cost. The IP-suite has eg for the time being no mechanism for meeting hard real time requirements.

SOA implemented as web-services imposes a substantial overhead, which means that the load on communication channels and on computer nodes is substantial.

The adherence to the general architectural principles may constrain the choice of technologies, acquisition practices and introduction of new systems.

Table of Contents

Abstract	iii
Summary	v
Table of Contents	ix
List of figures	xi
1 Introduction	1
1.1 The Objective of this Part of the Work (WP3).....	1
1.2 The Method Used to Produce the Target Architecture.....	1
1.3 The Target Architecture and Architectural Views	3
1.4 This Report.....	3
1.5 Relations to Other Work	4
2 General introduction to IT Architectures.....	7
3 DEFCOMM Reference Model and Related Concepts.....	9
3.1 Communication Reference Model.....	10
3.2 Information Systems Reference Model.....	13
3.3 Examples of Use of the DEFCOMM Reference Model.....	16
3.4 Definition of Terms, Terminology	18
4 General Principles and Non-Functional Requirements.....	21
5 Communication Architectural Views	23
5.1 Local, Regional and Global Communication Subsystems	23
5.1.1 The local subsystem.....	25
5.1.2 The Regional and National Subsystem.....	26
5.1.3 The Global Subsystem.....	28
5.1.4 Concluding Remarks on Subsystems.....	28
5.2 IP-Convergence.....	29
5.2.1 Gateways	30
5.2.2 IP-tunnel	32
5.2.3 VHF-example	33
5.2.4 Concluding remarks on IP-convergence.....	35
5.3 A Global Information Network	36
5.3.1 Transmission layer communication.....	37
5.3.2 NBO aspects	38
5.3.3 Concluding remarks on the global information network	38
5.4 Quality of service (QoS)	39
5.4.1 Background.....	39
5.4.2 Introduction	39
5.4.3 End-to-End QoS	40
5.4.4 Resource allocation.....	40
5.4.5 QoS architecture	41
5.4.6 Heterogeneous networks.....	41
5.4.7 Concluding remarks on QoS.....	43
5.5 Security	44
5.5.1 Availability	44
5.5.2 Cryptographic methods.....	46
5.5.3 Confidentiality	46
5.5.4 Access control.....	48
5.5.5 Security aspects of NBO.....	48
5.5.6 Concluding remarks on the security architectural view.....	49
5.6 Network Management	50
5.6.1 Network management concepts and objectives	50
5.6.2 Network Management reference model as a layered structure	51
5.6.3 Key Enabling technologies and protocols.....	52
5.6.4 Transition towards SOA	53
5.6.5 Concluding remarks.....	54
5.7 Addressing and routing	55
5.7.1 Addressing and routing in the DEFCOMM Reference Model	55
5.7.2 Addressing mechanisms and functions.....	56
5.7.3 Routing Mechanisms and Functions.....	57

5.7.4	Concluding Remarks on Addressing and Routing.....	60
5.8	Network Based Operations (NBO).....	61
5.8.1	Information Network.....	61
5.8.2	Sensor Network.....	62
5.8.3	Engagement Network (effector network).....	63
5.8.4	Concluding remarks on NBO.....	64
5.9	End-to-end Communication.....	65
5.9.1	Concluding remarks on the E2E architectural view.....	66
5.10	Communications Evolution.....	67
5.10.1	Snapshot 1, Initial architecture (today).....	67
5.10.2	Snapshot 2, Pre-NBO architecture (mid-way 1).....	68
5.10.3	Snapshot 3, NBO prepared architecture (mid-way 2).....	68
5.10.4	Snapshot 4, NBO supported architecture (target).....	69
5.10.5	Concluding remarks on evolution.....	70
5.11	Mobility.....	71
5.11.1	Concluding remarks on mobility.....	72
5.12	Other Communication Architectural Views.....	73
6	Application Architectural Views.....	75
6.1	Service Oriented Architecture (SOA).....	75
6.1.1	SOA Introduction.....	75
6.1.2	Service Implementation.....	77
6.2	Applications Evolution.....	81
6.3	Services and applications in NBO.....	83
6.4	Information Management.....	84
6.5	Naming services.....	84
6.5.1	Addressing in a Service Oriented Architecture environment.....	84
6.6	Application Security.....	85
6.7	Some Other Application views.....	86
7	Synthesis- Bringing It All Together.....	87
7.1	IP contra non-IP and other forms of dependence.....	87
8	General Aspects of the Architecture of Defence ICT systems.....	89
8.1	IP as protocol for Communication Convergence.....	89
8.2	The use of other protocols than IP as protocols for convergence.....	89
8.3	Gateways in general terms.....	90
8.4	Target architecture compliance with communication requirements.....	91
8.5	Concluding remarks on general aspects of the proposed architecture.....	91
9	The Target Architecture (top-level).....	93
9.1	Top-Level Target Architecture.....	93
9.1.1	General Top-Level.....	94
9.1.2	IP Top Level.....	95
9.2	Defence Information Systems.....	97
9.2.1	Non-SOA and Non-IP Information Systems.....	98
9.2.2	IP-compliant Information Systems.....	98
9.2.3	SOA-based Information Systems.....	98
9.3	The IP Communication Infrastructure.....	99
9.3.1	The IP-Infrastructure as Networks of Networks.....	100
9.3.2	The basic network.....	100
9.3.3	The IP-Infrastructure with the Transmission Mechanisms.....	101
9.3.4	The IP-Backbone and the Dynamic Infrastructure.....	102
9.3.5	Concluding Remarks on the Top-Level Target Architecture.....	106
10	Conclusions and recommendations.....	107
10.1	Recommendations Concerning Architectures and Evolution.....	107
10.2	Communication and Networks.....	108
10.3	Integration of Applications.....	108
10.4	Caveats.....	109
	References.....	111
	Appendix A: Enabling Technologies for Network Management.....	113
	Appendix B: Web-Services in Perspective.....	117
	Acronyms.....	119

List of figures

Figure 1-1: The overall method applied in the DEFCOMM work	2
Figure 3-1: DEFCOMM Reference Model.....	9
Figure 3-2: Communication part of DEFCOMM reference model – some functions and examples.....	12
Figure 3-3: Information System part of DEFCOMM reference model – some functions and examples	15
Figure 3-4: Use of DEFCOMM reference model for MIP and TP2K.....	16
Figure 3-5: Use of DEFCOMM reference model for network of networks	17
Figure 3-6: The DEFCOMM reference model applied to different abstraction levels	17
Figure 5-1: Communications subsystem view, conceptually and hierarchically	25
Figure 5-2: Examples of the local subsystem with possible technologies	26
Figure 5-3: Regional subsystem with example components.....	27
Figure 5-4: Global Communication Subsystem with IP-tunnels or IP-providers.	28
Figure 5-5: IP-convergence layer interworking with other networks/applications.....	29
Figure 5-6: IP-network of networks - Gateways used for connectivity to other networks	30
Figure 5-7: The IP-convergence architectural view	31
Figure 5-8: Example of gateway based data exchange between different devices	32
Figure 5-9: Integration of different transmission mechanisms	33
Figure 5-10: Tunnelling of IP-traffic through Link16 TDL	34
Figure 5-11: VHF Example – Gateway for VoIP	34
Figure 5-12: VHF Example - Tunnel of IP-traffic through VHF radio	35
Figure 5-13: Examples of communication technologies in a global information network.....	36
Figure 5-14: Main components of QoS at the Convergence layer.....	42
Figure 5-15: Example of domain partition in order to control availability	45
Figure 5-16: Examples of the positioning of crypto devices	47
Figure 5-17: NM basic Architecture.....	51
Figure 5-18: Layered NM functions related to DEFCOMM reference model.	52
Figure 5-19: Network management referenced to SOA view	54
Figure 5-20: Addressing and routing within DEFCOMM reference model.....	55
Figure 5-21: Applying various addressing strategies	57
Figure 5-22: Hierarchical relationship of the OSI Routing Architecture.....	59
Figure 5-23: The Information Network Architecture	61
Figure 5-24: Sensor Network architecture.....	62
Figure 5-25: Engagement Network architecture.....	63
Figure 5-26: End-to-end communication between defence and non-defence enterprises	65
Figure 5-27: Initial Architecture (snapshot 1)	67
Figure 5-28: Pre-NBO Architecture (Snapshot 2)	68
Figure 5-29: NBO prepared Architecture (Snapshot 3).....	69
Figure 5-30: NBO supported architecture (Snapshot 4)	69
Figure 5-31: Mobility supporting architecture.....	72
Figure 6-1: The three types of components in an SOA [3] and the contract	76
Figure 6-2: Service composition and orchestration (adapted from [Ref. 3])	78
Figure 6-3: Information System part of the DEFCOMM reference model in more detail.	81
Figure 6-4: Technology development and roadmap	82
Figure 6-5 The SOA approach to NBO	84
Figure 9-1: General Top-Level architecture	94
Figure 9-2: IP Top-Level Architecture	95
Figure 9-3: Application types interface to communication infrastructure	97
Figure 9-4: IP-applications with integration layer as interface to communication	98
Figure 9-5: Unified service.....	99
Figure 9-6: IP networks of networks	100
Figure 9-7: Example of a basic network as building block	101
Figure 9-8: Convergence as overlay on all transmission mechanism.....	102
Figure 9-9: Example with IP-backbone and dynamic infrastructure	103
Figure 9-10: Example of IP-backbone based on current networks.....	104
Figure 9-11: Example of IP-backbone segmentation	105

1 Introduction

This report describes the target architecture for ICT Systems in the Danish Defence¹ (~ Danish Armed Forces). The target architecture is a result from the analyses of selected scenarios (see DEFCOMM WP1 [Ref. 1]) and the requirements on the information and communications (see DEFCOMM WP2 [Ref. 2]). This report is the third and final work package of the DEFCOMM work (DEFCOMM WP3); - however, the three work packages should be regarded as a unified whole.

The DEFCOMM work shall support the transformation in which the Danish Defence is heavily engaged. The transformation involves in the technological arena a transition from the platform centric operations towards Network Based Operations (NBO). Another important trend is the fusion of administrative and operational systems, and the desire to be able to share information not only within the military area, but across ministerial boundaries and with suppliers and even private citizens. One prerequisite for this increased network centricity is the establishment of a networked information infrastructure. The target architecture is a blueprint for the infrastructure as we want it to be in a not too distant future, and is therefore a guideline for architectural considerations, including preparation of system architectures and planning of the acquisition of ICT systems, both hardware (HW) and software (SW).

The DEFCOMM work is made at the Danish Defence Research Establishment (DDRE) in close co-operation with HQ Chief of Defence CCIS Staff (IS2), and the Royal Danish Defence College. The authors want to thank for the valuable comments which were received from other defence authorities during the work.

1.1 The Objective of this Part of the Work (WP3)

The objective of the DEFCOMM work is to propose the target architecture for the ICT systems of the Danish Defence. The target architecture is an overall coarse grained structural design that describes future, ie 10-15 years ahead, systems of systems. It thus identifies the main components and the relations between these components in the overall ICT systems infrastructure. This work will be a stepping stone towards a more detailed form of system architecture. The level of detail is chosen so that the target architecture will be relatively independent of technological details. A certain degree of durability can thus be assured.

1.2 The Method Used to Produce the Target Architecture

The basis for the production of the target architecture is:

- The scenarios and vignettes which are described in WP1 of the DEFCOMM work [Ref. 1].

¹ The term Danish Defence and Danish Armed Forces are used interchangeably in this report, - however both terms mean the same, ie authorities under Ministry of Defence (MOD), including Defence Command Denmark, Home Guard, Danish Emergency Management Agency (see section 3.4 for more details).

- The functional requirements for communications and interoperability identified in WP2 of the DEFCOMM work [Ref. 2].
- A number of legacy systems which in some incarnation will exist in the time frame of this work. Legacy systems are otherwise only taken into account where necessary and to the degree they do not counteract the overall goals of the target architecture.
- A number of guiding principles such as the use of COTS, loosely coupled subsystems and overall application of a service orientation. Otherwise financial aspects are not considered.

The overall method is illustrated in Figure 1-1. The vignettes of the scenarios in WP1 are used to formulate requirements on information, and on ICT systems (WP2). These form the basis for the target architecture work (WP3). WP3 can be applied when the more detailed form of system architecture is to be developed.

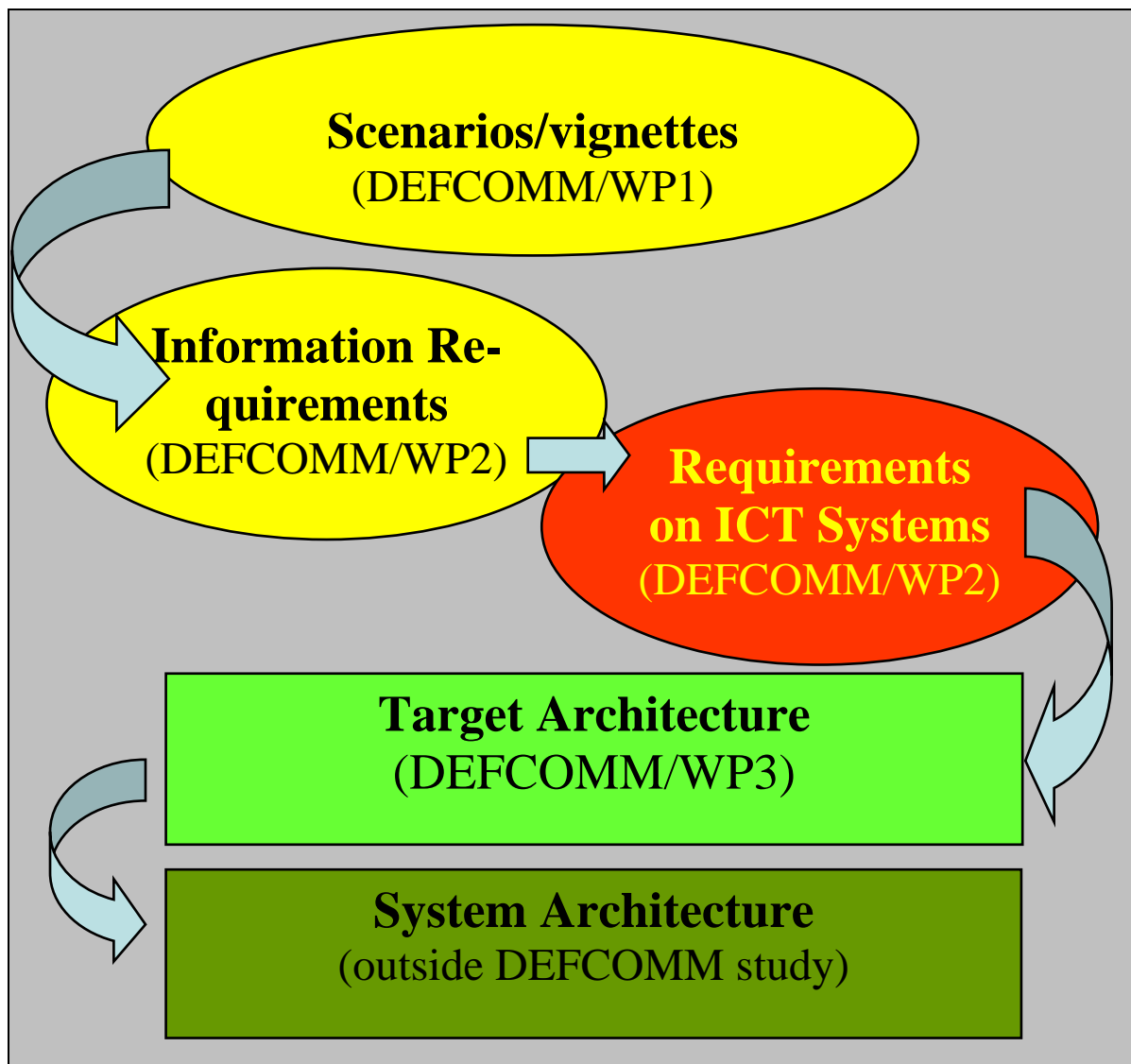


Figure 1-1: The overall method applied in the DEFCOMM work

The target architecture is a high level blueprint of the future system of systems. It is a goal that is to be worked towards in a time period. Therefore there are limitations both in the actual use of the target architecture, and in its actual contents. The most important issues are:

- The level of detail reflects to some degree the time available for this work. In a few cases detailed descriptions are included, mainly for proper consolidation of the target architecture. Specific examples are used for consolidation purposes as well.
- The target architecture is not to be used as an acquisition plan. It is to be considered as a guide to assure a directed development of a form of system architecture, but also as overall guidelines for acquisitions.
- The architecture does not point to specific products, and concrete standards are only included when they are crucial for the target architecture. In any case, the target architecture will give indications of types of products and of where it is necessary to apply standards.

1.3 The Target Architecture and Architectural Views

We have organised the work with the production of the target architecture in 4 steps. These are:

- Development of a reference model. This includes the necessary concepts and a vocabulary necessary for the formulation of the architecture. The reference model serves both the purpose of communicating the results and of a conceptual framework.
- Development of a number of architectural views directly related to the requirements derived in WP2. The architectural views do not necessarily only cover one aspect of the target architecture, but are aggregates compiled to map the requirements.
- Concatenation and analysis of the architectural views to reveal forms of dependences and constraints. This is a bottom-up approach to the target architecture.
- Development of the target architecture itself in a top-down manner, where the architectural views form the constituent parts.

The description of each architectural view and hence the number of architectural views have been chosen so that each of them represents an essential property or attribute of the information and communication systems of the Danish Defence.

1.4 This Report

The first chapter of this report contains an introduction to the work and the method applied.

Chapter 2 contains a general introduction to the concept of ICT system architectures. The main different types of architectures are defined, and the purposes of establishing such architectures are briefly iterated. The relation between the architecture and the reference model is also discussed.

In chapter 3 the DEFCOMM reference model that is used throughout the work is established. The concepts and vocabulary are defined, and the DEFCOMM reference model is compared to other recent models.

Chapter 4 introduces the guiding principles that we use, when establishing the target architecture. These general principles will be constraints on the architecture, and they act as a set of non functional requirements, which must be fulfilled.

The target architecture for communications consists of a number of architectural views, each of which deals with a category of requirements. Chapter 5 defines and describes these architectural views.

The target architecture for applications also consists of a number of architectural views. One of the guiding principles for the architecture at this level is a loose coupling between components (services). One way of exploiting this principle is by use of SOA, which is described in chapter 6. Also, in chapter 6 we briefly look at other architectural views related to applications and services.

Chapter 7 is a synthesis of chapters 4-6. It brings all the architectural views together and it contains a number of discussions of selected aspects.

In chapter 8 a number of general consequences of applying the target architecture are discussed, and its general properties outlined. It is further shown, that the architecture is in accordance with work in NATO and some of the guidelines from the Ministry of Science, Technology and Development. The applicability to NBO and the interoperability requirements are demonstrated.

The overall target architecture is exposed in Chapter 9.

The final chapter of the report, chapter 10, contains a number of conclusions and recommendations for further work.

1.5 Relations to Other Work

The ICT architecture serves as a blueprint, or an overall structural design, for a system. In this case the system is the overall coherent system that is composed of most of the ICT systems under the umbrella of the Danish Ministry of Defence. The main reason for having the ICT architecture now is the need for making all the component systems work together but still maintain their autonomy. This cooperative autonomy, which is based on a loose coupling between systems, facilitates sharing of data, information and services. The emergence of NBO is one example of this, another is the work done under the auspices of the Ministry of Science, Technology and Development on a common architecture for all state agencies [Ref. 12] and [Ref. 14]. Similar considerations have been made in many other nations (see eg [Ref. 17]) and in NATO and the EU.

In NATO, work on a technical architecture has been conducted by NOSWG [Ref. 10] in accordance with the NATO Architectural Framework (NAF) [Ref. 7]. NAF is heavily influenced by the US DoD work on Joint C4ISR architecture [Ref. 8]. The NOSWG work on the technical architecture was conceived before the decisions on moving towards Network Enabled Capabilities were made, and thus it does not fully exploit the opportunities in network centrality.

In Denmark, work on the communications target architecture for the Army was started in 2004, and many of the concepts and the methodology used in this work have been taken over from that [Ref. 6]. The work for the Army looks at the communication aspects from a NBO point of view, and recommends convergence through a network of networks based on the IP-suite. One main difference from that work is that in the present work, we put much more emphasis on the applications and their integration. The results from the army work are totally in accordance with the results of the DEF COMM work.

Further, in the national military area, joint (ie tri-service based) work on NBO has been started. One result of this is a report that among other things outlines an action plan for the Danish Armed Forces [Ref. 5]. Furthermore a conclusion from that report is that the technical architecture is one major stepping stone for obtaining an NBO capability in Denmark. Similar conclusions have been reached in the US and in NATO (eg [Ref. 18]). As a part of this national work, all the three services have separately conducted studies on their entrance into the NBO era (eg [Ref. 19], [Ref. 20]). The national studies take into account earlier work on Command and Control Systems (C2CS) done both at the service level, and jointly [Ref. 21].

In NATO, the trend towards network centricity has led to the NNEC Feasibility Study which outlines scenarios and a roadmap for the NATO transition to Network Enabled Capabilities. The present work takes into account the results from the NNEC Feasibility Study, as they appear in the current version [Ref. 4].

TACOMS Post 2000 ([Ref. 12]) is a seminal work that outlines the technical basis for tactical communications in NATO, and its connection to national assets. Although most of the TACOMS Post 2000 does not take into account the central position of an overarching communication network, the study contains much useful information. The present work is heavily influenced by TACOMS Post 2000, and is at major points in accordance with it.

In the Army, work on high level interoperability between command and control systems was conducted in the Army Tactical Command Control Information Systems (ATCCIS) project. This work has subsequently been taken over by the Multilateral Interoperability Program (MIP) and the NATO Data Administration Group (NDAG). The result of the MIP work is among other things information exchange data models that allow semantic interoperability between national C2 systems [Ref. 21], [Ref. 22]. Denmark follows this work closely, and the results are applied nationally. This has led to discussions on whether a common national data model should be introduced [Ref. 16].

It has been decided that Denmark will use Link 16 in all three services. To facilitate the introduction of Link 16, a study is being conducted at the Danish Defence Research Establishment (DDRE) [Ref. 23]. This study deals both with technical and organizational aspects. Link 16 will remain, for many years, one of the contributors to both interoperability and net centricity in the Armed Forces. Therefore results from the DDRE study are incorporated in this work.

2 General introduction to IT Architectures

In this chapter, we give a general description of the concept of ICT System architectures. In particular we define the term target architecture.

Architecture is a structural design. This means that architecture is a description of a system in terms of its components, their relations and their interfaces. Also interfaces to other systems are identified. There are many kinds of architectures, because they are depending on the purpose, the level of detail, a certain category of components, a certain set of relations and a snapshot or a time span. All this has made the concept of architecture ambiguous, and unfortunately misused. To use the term meaningfully, some choices of the purpose of the architecture must be made explicitly.

ICT system architecture is often described in terms of three views or specific types of architectures. There seems now to be a consensus about the terminology. NATO and the US operate with three kinds of views ([Ref. 7] and [Ref. 8]). An architecture view is defined as “a representation of a whole system from a particular viewpoint, ie from the perspective of a related set of concerns. The three views are:

- The *operational view* is “a description of the tasks and activities, organisational and operational elements, and information flows required to accomplish or support an operation”.
- The *system view* is “a description, including graphics, of systems and interconnections providing for, or supporting, system functions”.
- The *technical view* is “the minimal set of rules governing the arrangement, interaction, and interdependence of systems parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements”.

With the introduction of SOA, it will be necessary to define a fourth view representing the service layer of the architecture. Introducing a service view will effectively decouple the operational view from the system view, and will therefore assist in aligning business requirements on the IT resources. The service view is expected to contain a number of templates, which govern the design of service views. A *service view* could eg consist of templates describing:

- A mapping between operational requirements and services.
- A description of service orchestration as well as service aggregation and sequence requirements.
- The service composition description necessary to model the reference model application layered service orchestration.
- A description of the service hierarchy.
- A list of service definitions.

When additional knowledge and experience with SOA has been developed, it will be appropriate to define additional service view templates, each illustrating additional aspects of SOAs.

In the DEFComm work, we mainly use the system view. The system view focuses on components which in their own right may be communication systems, major information systems and the relations between systems. In this view, the interfaces are also identified.

The architecture described in this document is composed of a number of architectural views. Each view describes primary aspects from the system view, but also aspects from the technical view.

In this report we use a number of terms for different types of architectures. Each type serves a specific purpose.

The **target architecture** is a high level structural design, which serves as a fix point for the evolution or evolutionary development of a system for a number of years. The target architecture of the DEFCOMM work deals with a time span of 10 to 15 years from now. The main purposes of the target architecture are:

- To make sure that the present and future operational requirements on ICT systems can be met.
- To ascertain that communications equipment as much as possible fits together and is as similar as possible. To a limited degree also legacy systems are regarded.
- To assist in making equipment interoperable and able to support NBO.
- To increase the quality of the total systems of system that forms the ICT infrastructure.
- To facilitate the use of COTS components.
- To guarantee that acquisitions both from a usability and technological point of view have a reasonable life time.
- To make the acquisition and maintenance processes easier, less costly and faster.

It must be stressed, that the term target architecture is not identical to the similar NATO term, which describes a detailed, project related system implementation target (Type B cost estimate (TBCE)). The target architecture described in this document has a stronger resemblance with the NATO concept overarching architecture.

The **system architecture** is defined as an instantiation of the target architecture. It may thus directly serve as a guidance and part of a requirement statement for acquisition and maintenance.

An **architectural view** deals in this report with specific aspects of the target architecture, viewed from an operational, a system or a technical point of view. The architectural view may thus be at different levels of detail depending on its concrete purpose.

It is important to have a common conceptual framework when discussing architectures. For that reason we introduce a reference model for the defence ICT systems in chapter 3. The **reference model** presents the main concepts, their relations to each other, and it gives thus a structure and shows the dependences between services, protocols and interfaces. This conceptual framework is adapted to the task at hand, ie the development of the target ICT architecture. Basically the reference model is a layered model, including a transmission layer, a convergence layer, an integration layer and a service layer. This model is different from the OSI 7 layer model in many respects. This reference model is able to cope with the system of systems which are the nucleus of this work, and also non-OSI compliant protocols like the ones used in tactical data links and on the Internet.

3 DEFCOMM Reference Model and Related Concepts

In this chapter, a layered reference model for the communication infrastructure and the application structure of the Danish Defence is introduced. The model is denoted **Danish Defence Communication Reference Model** (short: **DEFCOMM Reference Model**), and the purpose is to define a structured framework and terminology for a description of the target architecture. This model includes relevant key technologies, and it points towards a converged network infrastructure as the communication infrastructure, and SOA as the application structure. The converged network and SOA are the cornerstones of the target architecture.

The total DEFCOMM reference model with both the communications side and the information systems side is illustrated in Figure 3-1 with the colour codes used throughout this report.

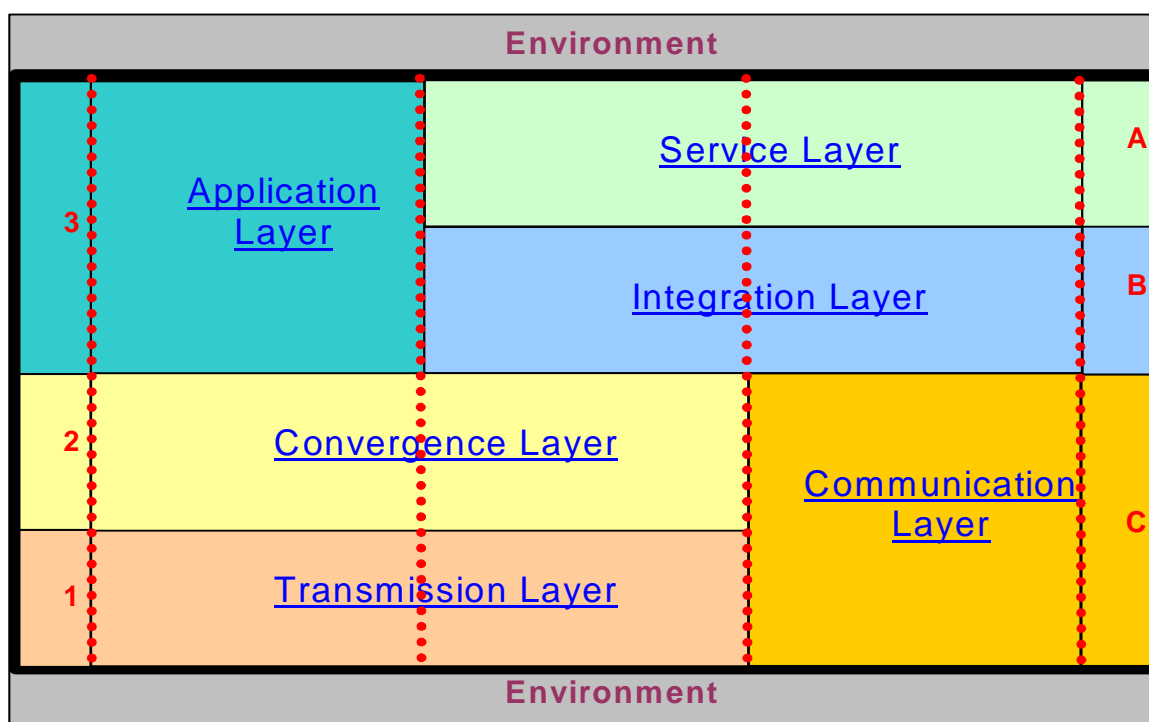


Figure 3-1: DEFCOMM Reference Model

The DEFCOMM reference model is a four layer model as illustrated in Figure 3-1. The layers are denoted transmission, convergence, integration and service- However for most purposes in this report; we look at the model from two perspectives, a communication side as illustrated in the left side of the figure or from an information system/application side as illustrated in the right side of the figure. Those two sides are described separately as three layer models in sections 3.1 and 3.2, respectively².

From the **communications side**, the reference model has three layers, and all communications functions can be related to these layers. The model is specifically well

² It should be noted that the communication part of the DEFCOMM reference model is identical to the reference model used in the architecture study for the Danish Army [2]. However, in the army study the level of detail at the application layer is different.

well suited to describe heterogeneous network of networks, and a similar structure has been used in the TACOMS Post 2000 specifications, etc. The three layers are shown to the left in Figure 3-1 (layers 1-3) and denoted transmission, convergence and application layers. Note that the application layer is the same as the integration and service layers of the application structure (seen from the information system side), but from the communication side the application structure is seen as one layer only.

From the **information systems (or application) side**, the reference model has three layers as well, and all information systems functions can be related to these layers. This model is specifically well suited to describe a realisation in the form of SOA with a loose coupling between the services. The three layers are shown to the right in Figure 3-1 (layers A-C) and denoted service, integration, and communication layers. Note that the communication layer is the same as the convergence and transmission layers, but from the application side the communication infrastructure is seen as one layer only.

In Figure 3-1, the **environment** is shown both at the top and the bottom. The environment at the top consists of users using the ICT systems, including persons with MMI, sensor-heads for data acquisition, and effectors to affect the physical world. The environment at the bottom indicates that the transmission mechanisms may be influenced by the physical environment, eg landscape and weather.

3.1 Communication Reference Model

The three layers in the communication part of the DEFCOMM reference model are defined as:

- Layer 1 (lower layer): *The **transmission layer*** contains all the transmission mechanisms that can be used for the transfer of data, both as direct physical connections and as dedicated networks. This includes but is not limited to fixed trunks and links, radio links, satellite links, cabled connections, fibre optical links and microwave links. One example is the lower layers of the Danish Integrated Information Network (FIIN).
- Layer 2 (middle layer): *The **convergence layer*** is the glue that from a communications point of view makes the network of networks appear as one seamless pool of facilities for information exchange. It contains the protocols that use the transmission layer, but in a way that makes the functions of the convergence layer (and above) independent of the transmission layer. A strong candidate for the main convergence layer protocol is the IP-suite with IPv6. This will of course require that all applications must have the ability to use, ie communicate via, the IP-suite.
- Layer 3 (upper layer): *The **application layer*** is where all user systems, services and applications reside. These services are both communication services which are part of the communication infrastructure, and application services that are furnished by users or communities of interest. A few examples of upper layer services are DEMARS, Coastal Radar sensor information, Voice over IP, and systems for document handling.

All communications functions can be related to the three layers defined above. Some functions are relevant at all layers. These are (network and information) management, Quality of Service (QoS) and security:

- Network Management (NM) is both applied at each layer and integrated across all layers.
- QoS is important at all layers, because QoS at a higher layer is depending on QoS at lower layers. Higher layers may compensate for lack of QoS at lower layers, but at a cost. Compensating mechanisms may eg be buffering, caching or intelligent error correction. There are three different components that relate QoS to the reference model:
 - QoS service level agreement (SLA). Applications which need a QoS connection may use resource reservation through the convergence layer.
 - QoS signalling (protocol) to coordinate QoS issues through the whole network structure.
 - QoS policy, which must control how QoS is administered with regard to the available resources.

These three components are placed at the convergence layer in the reference model. Their main function is handling of QoS across heterogeneous transmission mechanisms at the transmission layer.

- Security in the shapes of integrity, availability, confidentiality and non repudiation is found at all three levels. As for QoS there are cross forms of dependence between the layers.

Dedicated systems such as tactical data links play at least two parts. One is acting as an autonomous communication system, which by itself covers all three layers in the reference model. Another part is as yet another transmission mechanism, where higher order communication is tunnelled through the data link. This will usually be a costly way of achieving connectivity, but it is certainly a possibility in a converged network infrastructure.

Some of the functions and examples are shown in Figure 3-2.

It is important to note, that the three-layer DEFComm reference model (communications part) is not directly related to the well-known OSI- 7 layer reference model; however, in some cases a direct mapping is possible. The DEFComm layered model, however, is so flexible that it can accommodate other communication models, both OSI and non-OSI.

The DEFComm reference model can be used at several levels, because heterogeneous networks can be used as each others' transmission mechanism. It is possible within the reference model to view one or more as transparent, - for example a virtual private network (VPN) can be viewed as a (transparent) transmission mechanism between two local IP-based networks. A network can then be viewed both as an application transport service (layer 3) and as a transmission mechanism, - depending on the context. This can be done a number of times, - in principle recursively. An example is described in section 3.3.

The reference model is widely applicable at all levels of the communication system, and the model can be used down to the wanted level of detail. All components in the target architecture must be related to a layer in the reference model. A corresponding model can be used for the system architecture. However, in that case it will be necessary to look in more detail at the interfaces between the layers.

Some functionalities to be applied on all layers	Layer	Some functionalities specific for each layer		Examples of functions	Examples of dedicated systems
<p style="text-align: center;">Network Management</p> <p style="text-align: center;">Security such as availability and access control</p> <p style="text-align: center;">Quality of Service</p>	<p style="text-align: center;">Application layer [3]</p>	<p>Defence Services/Applications/Facilities.</p> <p>Communication related applications:</p> <ul style="list-style-type: none"> • Security such as E2E confidentiality (PKI) and access control • Network management 		<p>Video Transmission</p> <p>Telephony</p> <p>Telemetric</p> <p>Applications based on SOA</p>	<p>Tactical datalinks (TDLs)</p> <p>Radio systems</p> <ul style="list-style-type: none"> • HF • VHF • ...
	<p style="text-align: center;">Convergence layer [2]</p>	<p>Convergence protocol</p> <p>Quality of Service</p> <ul style="list-style-type: none"> • SLA • Signalling • Policy <p>Addressing/Routing</p> <p>Mobility</p> <p>Confidentiality (network)</p>		<p>Protocols</p> <ul style="list-style-type: none"> • IP, ATM, other standards <p>QoS for streaming data</p> <p>Addressing./Routing</p> <ul style="list-style-type: none"> • Hierarchic addressing/routing • Proactive/reactive routing <p>Mobility of terminals/network</p> <p>Mobility management</p> <p>IP-cryptography</p>	
	<p style="text-align: center;">Transmission layer [1]</p>	<p>Transmission mechanisms such as:</p> <ul style="list-style-type: none"> • Trunks • Links • Transmission networks • VPNs <p>Security</p> <ul style="list-style-type: none"> • Confidentiality (link) 	<p>Tactical datalinks (TDLs) as transmission mechanisms</p>	<p>IP-network</p> <p>Wireless network (ex. WiFi, Bluetooth)</p> <p>Infrared link</p> <p>Cellular network (ex. GSM, UMTS)</p> <p>MANET (ad-hoc network)</p> <p>PSTN/ISDN</p> <p>X.25</p> <p>ATM-network (ex. DEOS 2000)</p> <p>SATCOM</p> <p>Radio network (ex. VHF, UHF)</p> <p>FIIN-infrastructure</p> <p>Crypto equipment</p>	

Figure 3-2: Communication part of DEFComm reference model – some functions and examples

3.2 Information Systems Reference Model

The three layers in the information systems part of the DEFComm reference model are defined as:

- Layer A (upper layer): *The **service layer*** contains all the military services to be produced (~ provided) or consumed. All services must have a well-defined interface to the integration layer (~ middle layer), but the services themselves can live in an autonomous way thus making them able to support all the needs of the Armed Forces. All data models will reside at this layer to ensure interoperability between applications, eg Joint C2 Information Exchange Data Model (JC2IEDM). The services can be either COTS applications or can be dedicated military applications. However, the services with a well-defined interface towards the integration layer make it possible to have the loose coupling between services. In the NBO environment the sensors, effectors, and C2-systems will be the service producers or consumers. A few examples of upper layer services are raw or processed sensor-data, fused sensor-data, commander intentions, detailed orders from HQ, COP, status of weapon, and launch commands.
- Layer B (middle layer): *The **integration layer*** is a logical layer which ensures that the services from layer A are interoperable as producers and consumers. This layer can be compared to the convergence layer in the communication part of the DEFComm reference model; - the integration layer is the glue that ties the services together in a loose coupling ensured by the well-defined interface. Examples include most of the IP-suite application protocols, - including HTTP, SMTP, and FTP. Also web-services like SOAP, WSDL, and UDDI reside at this layer. XML is an important integration standard as well.
- Layer C (lower layer): *The **communication layer*** is where all the network services from the communication infrastructure reside as they are seen from the integration layer. This means that information from service and integration layer in a seamless way can be transported by the network to make the information available where needed. A few examples of communication layer services are IP-networks, FIIN, wireless connection, and cabled connections.

The model with the three layers mentioned above is at a high abstraction level and therefore generally applicable. However, the model easily accommodates concepts such as component based systems and SOA for the Danish Armed Forces.

All information systems functions can be related to the three layers defined above. Some functions are relevant for more than one layer. Network management, security and QoS are cross concerns, ie they cover all layers, see Figure 3-2. Note that network management includes system management. Furthermore there are functions covering both the service and integration layers but not the communication layer.

These functions include:

- Transaction support, including recovery facilities.
- Information Management.
- Service Registry, ie facilities for providers to register a service, and consumers to discover services.

Some of the functions with examples are shown in Figure 3-3.

Information management includes all the services that are involved in capturing, storing and retrieving information. In a large inhomogeneous system of systems this is not a trivial task, which encompasses maintenance of metadata, including data models and directory information. At the lowest level, we find database management functions. These services all reside in the application layer of the reference model, and will not be further dealt with in this report.

Transactions are sequences of operations that have the following properties:

- Atomicity, i.e. they are either all executed, or none are executed.
- Consistency, i.e. they guarantee that data stores are left in a consistent state, or in a state as consistent as before the transaction,
- Isolation, i.e. the transaction is not disturbed by concurrent operations from other processes or transactions, and
- Durability, i.e. the results of the transaction is in principle available in all future.

Transactions are for security reasons important in many contexts, but they require many resources to perform. Transaction services reside in the application layer of the reference model and will not be further elaborated in this work.

Some functionalities to be applied on all layers	Some functionalities to be applied on service and integration layers	Layer	Some functionalities specific for each layer	Example of functions
<p style="text-align: center;">Network Management Security such as availability and access control Quality of Service</p>	<p style="text-align: center;">Information Management Transaction Service Registry</p>	Service layer [A]	Service Process: <ul style="list-style-type: none"> • Choreography • Orchestration Discoverable and invocable Services	Web Service Process: <ul style="list-style-type: none"> • Orchestration: WS-BPEL • Choreography: WS-CDL Services Implementation: <ul style="list-style-type: none"> • Application Servers (J2EE, WSIF)
		Integration layer [B]	Service Description Server Communication Transport Services	Service Description: <ul style="list-style-type: none"> • XML, WDSL, ebXML Server Communication: <ul style="list-style-type: none"> • SOAP, ... Transport service: <ul style="list-style-type: none"> • HTTP, SMTP, JMS, • WS-Reliable Messaging
	Communication layer [C]	Communication Services and Facilities. Application related communication functions: <ul style="list-style-type: none"> • QoS, Mobility, Availability, Confidentiality, Addressing, . . . • Transmission Mechanisms Management of: <ul style="list-style-type: none"> ○ Trunks, Links, Networks, VPNs • Use of TDLs 		

Figure 3-3: Information System part of DEFCOMM reference model – some functions and examples

3.3 Examples of Use of the DEFCOMM Reference Model

In this section a few examples of use of the DEFCOMM reference model are given.

The first example is the DEFCOMM reference model used to show the protocols and interfaces necessary to obtain net centricity in a system of systems based on a common data exchange model, JC3IEDM. This is an example where the DEFCOMM reference model can be directly related to the OSI- 7 layer model. This is illustrated in Figure 3-4.

DEFCOMM Reference Model	JC3IEDM based protocols (MIP)					TP2K OSI-stack	MIP over TP2K OSI-stack
Application layer	DACCIS, RDNCIS, NEC CIS Protocol and data conversions.						
	Message Exchange Mechanism (MEM)		Data Exchange Mechanism (DEM)				7 6 5
Convergence layer	Convergence protocol TCP/IP						4 3
Transmission layer	(Secure) Voice	Data	Mail	Real time applications	(Secure) Video	7 6 5	2 1
	TACOMS Post 2000 transport service					4	
	TACOMS Post 2000					3 2	
	Cables, optical fibres		Wireless (waveforms)			1	

Figure 3-4: Use of DEFCOMM reference model for MIP and TP2K

The second example shows how the communication part of the DEFCOMM reference model may be used recursively, in the sense that at a given abstraction level, the convergence may serve different purposes. This is illustrated in Figure 3-5, where a transport mechanism may be described as a “new” three-layer model. This new model can be viewed as a transparent transport service (~ tunnelling). The top level is an IP-network which uses an ATM-network as a tunnel (~IP over ATM). This ATM-network then uses telecommunication (telco) with SONET (or SDH) as a tunnel. At the low level, fibre optic cables are used as the transmission mechanism for SONET.

A third example is the use of SOA. By using Web-services this is indeed feasible on an IP converged network, but the web-services will also serve as integration layer (similar to the communication convergence layer) on the higher abstraction level of services.

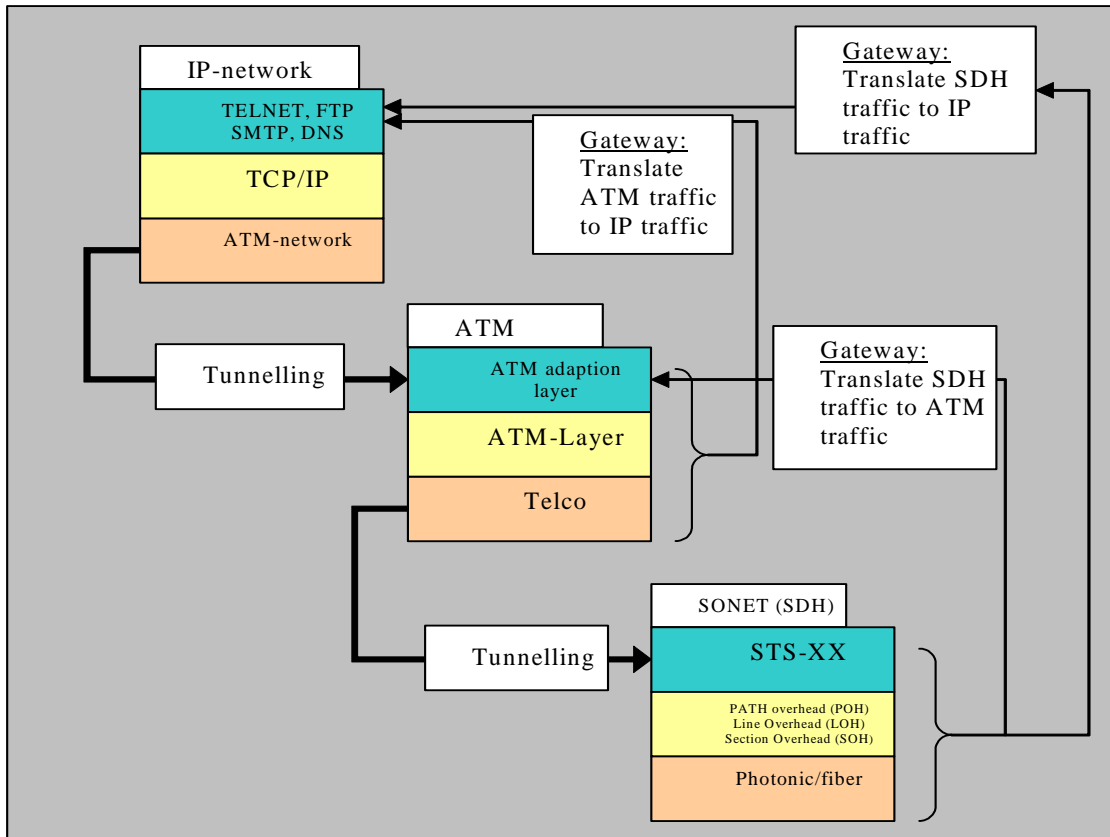


Figure 3-5: Use of DEFCOMM reference model for network of networks

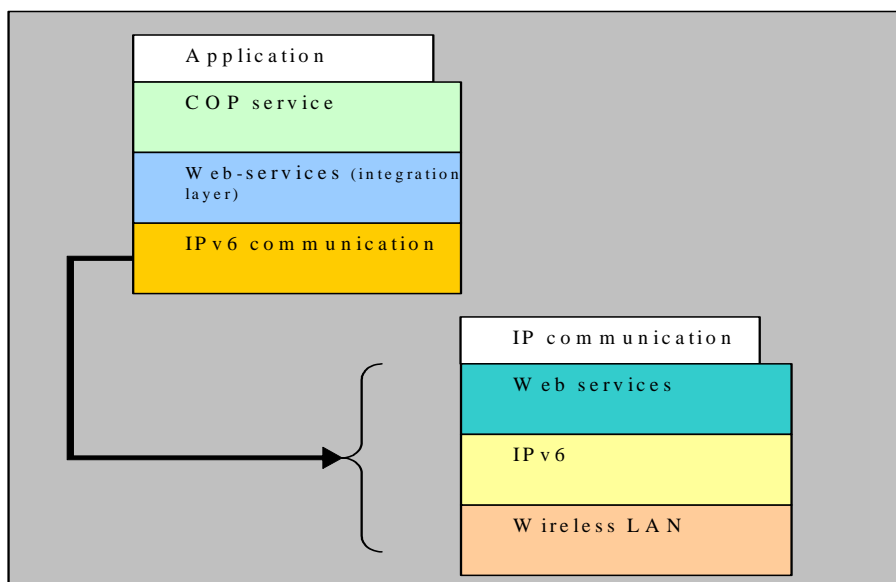


Figure 3-6: The DEFCOMM reference model applied to different abstraction levels

The recursive use of the reference shows that at different abstraction levels, the role of the layers will change. In the example in Figure 3-6 the web-services will act as an integration layer, ie all applications will be web-services and adhere to the appropri-

ate standards. At the next lower abstraction layer, the IPv6 is the glue that binds all nodes together.

3.4 Definition of Terms, Terminology

The most important terms are defined in the following list. The list is not meant to be complete, but it will serve as a useful starting point for reading the rest of this report.

Actor: The generic term used for active parts of the ICT systems and its environment. They may be processes or end users. Actors may be both service providers and service consumers. In this report actors are usually referred to as users.

Application Structure: The general term for the applications part of the ICT systems, ie the application structure includes all the components residing at the application layer of the DEFCOMM reference model.

Converged Network: This is a network where all communication is based on one protocol. In OSI-terms this convergence may take part at different layers. An example is the IP converged network where the IP is the convergence protocol.

Converged Network Infrastructure: A communication infrastructure based on a converged network.

Communication Infrastructure: The general term for the communications part of ICT systems, i.e. communication infrastructure includes all components residing at the communication layer of the DEFCOMM reference model.

Convergence: This is the process, where otherwise separate technologies gradually are fused, so that they form one conglomerate. One example is data communications and telecommunications. They were from their different origins considered as two separate disciplines.

Core-IP network: Is a network where the essential parts, i.e. the core, are based on the IP-suite.

Danish Armed Forces: A general term used interchangeably with *Danish Defence*.

Danish Defence: In this report this is the general term used for whole MoD area. It is used interchangeably with *Danish Armed Forces* and includes all authorities under the Danish MoD, including Defence Command Denmark (*Danish: Forsvarskommandoen*), Home Guard (*Danish: Hjemmeværnet*), and Danish Emergency Management Agency (*Danish: Beredskabsstyrelsen*). Also the Total Defence (~ Homeland Security) is included.

Edge-device: A general term used for all network devices connecting one network-system to another network-system. Examples are routers, gateways, firewalls, or security devices.

End-user: Denotes a person as part of the environment, see Figure 3-1.

ICT Systems: The general term for all defence Information and Communication Technology Systems. This includes Communication Information Systems (CIS) and administrative systems such as Management Information Systems (MIS).

Information Infrastructure: The same as *application structure*.

Information Systems: General term for systems at the application layer supporting the *users* of the ICT systems. Information systems include applications.

Infrastructure: Brief form of networked or communication infrastructure

IP-infrastructure: An infrastructure where IP is the convergence protocol.

IP-suite (or the IP-stack): Denotes the protocols where IP is the network layer protocol. It comprises among other things HTTP, SMTP, TCP, UDP and IP.

IP-telephony: This is voice over IP with add-on services for supporting traditional telephone systems.

Network device: A physical unit which can be connected to the network. Examples are terminals, routers, hosts, gateways, switches, or hubs. A network device can also be denoted a (network) node.

Networked Infrastructure: Denotes the part of the network which is the converged network, including the lower level transmission mechanisms. In the DEFCOMM reference model, this is the middle and low layers.

Network of Networks: A common term used to indicate that a network may consist of other interconnected networks. Together with *system of systems* this is the basis for NBO.

Network-system: A system of networks, ie just another general term for *network of networks*.

Service Consumer: A service consumer is a user of service offered by a service provider. Note: A consumer may also be a provider of a service. A consumer will be able to use a service without knowing anything of the inner workings of the service.

Service Level Agreement: Describes an agreement between parties. In SOA, it describes the contracts between a service provider and a service consumer (ie the interface between the two parties). However, the term is also used in other domains with a similar meaning.

Service Provider: A service provider is a *user* offering service to service consumers. All service may be implemented independently of the service level agreement, which constitutes the contract between a consumer and provider.

Service: A service is produced by functions residing at the application layer of the DEFCOMM reference model. A service is a useful activity or resource, which may be produced on demand or published without an explicit or a priori known consumer. Services may be produced by processes from other layers, but in that case we shall explicitly point that out.

Subsystem: In this report this term is related to the communication architectural view for local, regional, and global subsystems (see section 5.1).

System of Systems: A common term used to indicate that a system may comprise of other systems or subsystems. Together with networks of networks and *system of networks* this is the basis for NBO.

Terminal Equipment: A common way of denoting network units used as the CIS interface to the environment. In this context the CIS environment is persons interacting with the CIS through its MMI, where sensor-heads record data, or effectors affect the physical environment.

Transmission Mechanism: A transmission layer function, the purpose of which is to make exchange of information possible in a transparent way.

Transport Service: An application from the application layer. Such an application will draw upon services from the lower two layers. One example is Voice over IP.

Voice over IP (VoIP): The service of sending sound or voice across a network based on IP. We distinguish between VoIP and *IP-telephony*, where the latter also includes the normal telephone services expected in the plain old telephone system.

User: In this report the word user is used in a broad sense as a synonym for actor meaning any provider or consumer of information. This includes end-users (eg a soldier or a person), terminals (eg PDA or a PC), application (eg a telephony program), a process (eg a tracking algorithm or a time service), sensors (eg microphone or a radar), effectors (eg transmitter or weapon platform), military information systems (ex. DEMARS or BMS), etc.

User Terminal: Terminal equipment where the environment is a person.

4 General Principles and Non-Functional Requirements

In this chapter, we briefly clarify a number of governing principles for the target architecture. These principles span a width from common sense to best practice. They will be an important part of constraints for the architecture, and as such they will form a set of non-functional requirements. These requirements can not be directly derived from the scenarios of WP1, but they will a.o. be important for achieving a number of the functional (user) requirements of WP2. The non-functional requirements thus form a necessary and complementary set of principles, complementary to the user requirements.

Standards - The architecture shall implement as many functions as possible based on open standards, in terms of protocols, underlying technologies and methodologies. It is important to facilitate and encourage reuse and commonality both at component and at systems level. The access to services must be independent of the network type and the inner workings of the service. In this context, the IP-suite is of paramount importance.

Scalability - The converged network infrastructure must be scalable in the sense that it must be a simple task to add new capacities, services, applications and users to the structure. In principle, this should be possible on demand.

Location Transparency - The physical placement of users and resources must be transparent to the consumers and the producers of services. Functions that used to be only accessible in headquarters are to be available overall and for all legitimate users. This does not preclude a central management.

Open Architecture and Innovation - The use of an open architecture will facilitate cooperation or partnering between producing companies and the military users and acquisition people. The open architecture will encourage competition and prevent dependence on a single supplier. The use of proprietary and special military standards should be avoided. The architecture must itself be able to evolve and support the technological evolution.

Flexibility - An open architecture means an increase in the number of suppliers of functionalities, and the development of the system of systems will be dictated more by the users than by the commercial and military market. The roll-out or deployment of new functionalities in the form of eg services will be faster and easier, both in terms of geographical coverage and in terms of number of users. The converged network structure will favour a consistent span of services independent of the underlying transport mechanism. This will make it possible to choose the most appropriate transmission channel in a given situation.

Network Management (NM) - The open and converged network architecture will make it possible to monitor and control the whole network of networks by one team instead of having a number of independent and isolated groups taking care of networks and services. Because all resources are harboured on the same network, the exploitation of the resources can be efficient.

Quality of Service (QoS) - The converged network must be able to deliver a broad spectrum of QoS, which includes the support of time critical applications and isochronal services.

Reliability and Availability - The converged system of systems must have redundancy to maintain high availability of all critical resources.

Transmission Capacity - The networked infrastructure must offer the necessary capacity and signal processing to accommodate both voice and video applications, and the supply of timely information where necessary.

Security (Confidentiality and Data Integrity) - The core network must be black (ie encrypted), meaning that users must have the possibility of encrypting classified information. Data link encryption in parts of the infrastructure to increase the security should not be ruled out.

Control of Electrical Power - Parts of the communication system must apply technologies with low power consumption, including protocols that do not require frequent keep-alive signalling. This is particularly important for unmanned devices with a limited battery capacity.

Mobility - Mobility comprises the independence from geographical location and the ability to be operational when on move. It must be possible to establish ad-hoc networks to accommodate this and thus obtain communication without having to rely on eg a fixed infrastructure.

Loose Coupling - The principle of loose coupling between the components in the total system is important. Loose coupling means that the components expose coarse grained interfaces to the network, and that as much lifetime control of software objects and processes as possible is done locally, at the node where they reside. Communication between components is as a principle done via messages, and wherever possible by asynchronous (non-blocking) message passing eg via queuing systems. The loose coupling reduces the overall complexity and allows the components to evolve at their own pace. A change in technology in one component does not affect the other component. SOA is one method for obtaining loose coupling.

Network Basis - In all cases, the operations must be network based. The most important properties of the network centricity may be summarised as a movement from as-is to the desired out-come, to-be [Ref. 11]:

AS-IS (Today, Platform Oriented)	To-be (Network Based)
Platform based	Capability based
Point-to-Point	Net-centric
Stow-piped information and services	Shared information and services
Emphasis on systems and their functions	Emphasis on services

The movement towards Network Based Operations will have implications for all applications and for the architecture of both the communication systems and the information systems.

5 Communication Architectural Views

In this chapter we define and discuss a number of architectural views that together will form the target architecture for communication. The level of detail in the description of the views differs somehow from view to view depending on the presumed familiarity with the concepts and its importance in the overall architecture. This means that some of the views are dealt with in a generic manner, while others are very specific. The sequence in the description does not necessarily imply a priority. Further, each subchapter, ie each architectural view, is described so that it is possible to read it independently of the other subchapters. This means that there is a certain overlap between the different architectural views and their descriptions.

For each architectural view we describe:

- What is the specific purpose of this part of the architecture?
- What is the scope and environment, including its role in the DEFCOMM reference model?
- Which requirements are fulfilled by the view, and which requirements must it itself fulfil?

Most of the architectural views are analysed with regard to their properties, advantages and disadvantages. The expected technological evolution and its impact in the timeframe of this work are included.

The background for the communication architectural views is the information systems part of the DEFCOMM reference model (see Chapter 3). As shown in Figure 3-1 this part of the reference model consist of three layers (1-3) also denoted transmission-, convergence-, and application layers. The basic of the communication target architecture is the converged network with IP as the convergence protocol, and the transmission mechanisms to fulfil the specific requirements of the defence regarding security, robustness, quality-of-service, capacity, etc. These mechanisms and the converged network form a seamless communication infrastructure, and will be an important facilitator when implementing NBO.

5.1 Local, Regional and Global Communication Subsystems

The purpose of this section is to look at the communication system from a *geographical point of view*. The total communication system is split into local, regional and global subsystems as illustrated in Figure 5-1. This view has been selected because each of the 3 subsystems to an important degree uses its own communications technology. Furthermore, this makes the traceability back to scenarios and requirements (WP1 and WP2) more obvious, especially issues concerning information reach.

As an example of this partition of the communication space we consider the TA-COMS Post 2000 (TP2K) study [Ref. 12]. In T2PK, 4 subsystems for tactical communication are considered, namely a Local Area Subsystem (LAS), a Wide Area Subsystem (WAS), a Mobile Subsystem (MS), and a Management Subsystem (see eg STANAG 4637). LAS typically supports a headquarters (HQ), WAS gives connection between HQs, to the civilian infrastructure, and to strategic communication assets, while MS represents radio networks. The WAS functions as a communications backbone. In the DEFCOMM work, we consider mobility a general issue, and thus do not

deal with a dedicated mobile subsystem. From a technological point of view, there will be mobile components in all of the three other subsystems.

The scope of DEFCOMM is broader than tactical communication in the sense that we look at defence *and emergency services* ICT systems in a broad sense that includes applications.

The target architecture and the architectural views reflect the transition towards Network Based Operations (NBO), i.e. the systems of systems or network of networks concept. The local system consists of a number of smaller networks that are mainly dedicated for specific purposes. The target architecture shows how these subsystems may be integrated on a converged network based on the IP-stack, and it shows how the communication subsystem allows an integration of applications, mainly based on an SOA.

- The local communication includes internal communications (corresponding to the TP2K LAS) in platoons, groups, up to components of BDE or DIV HQs. We also include the purely localised communication such as personal area networks (PANs) and communications internal to platforms such as ships. The local subsystems will very often feed into the global subsystem, and it will be mediated by both cables and radio.
- The regional communication typically covers an area of the size of a classic division or a naval task force. The communication means will be a mixture of wireless, ie radios, and cabled equipment. A typical case is the DEOS 2000 area signal system used by the Danish Army.
- The global communication, corresponding to the TP2K Wide Area Subsystem (WAS) covers communications over large distances (Beyond Line Of Sight, BLOS). Typically media such as HF- radios and SATCOM will carry the communications. Communications from units deployed far from Denmark and other sorts of reach-back will be important aspects of this kind of communications. Most strategic communications will be under this umbrella.

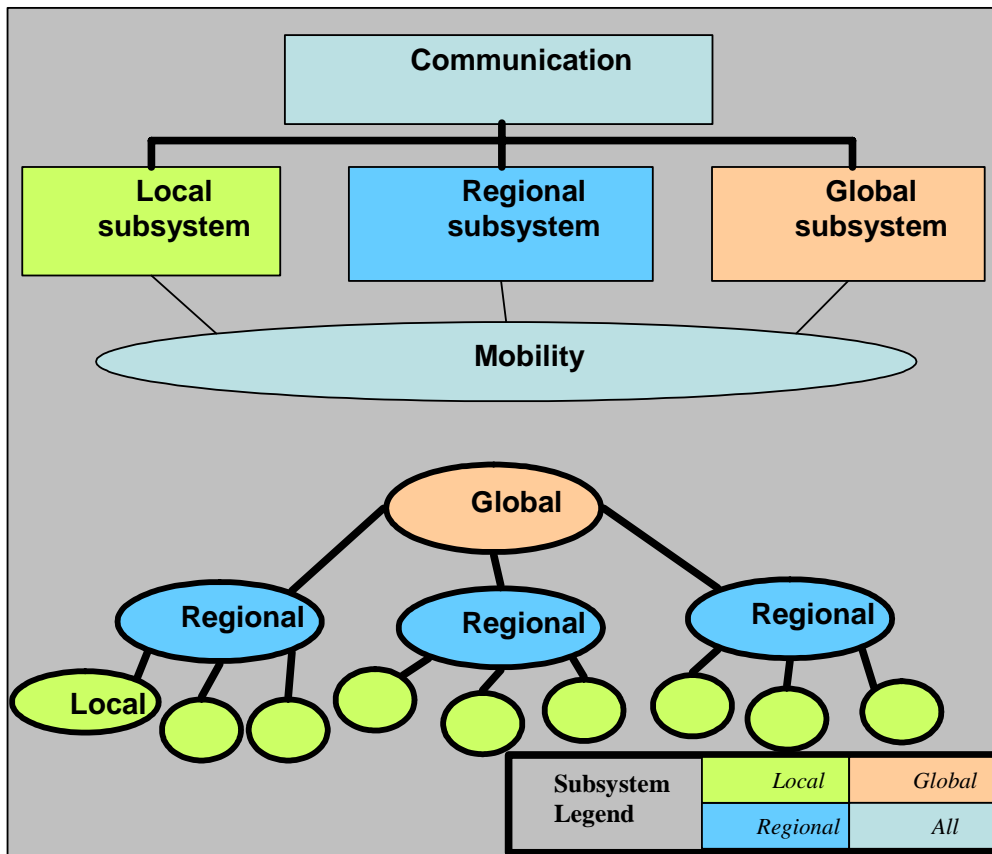


Figure 5-1: Communications subsystem view, conceptually and hierarchically

The total system may in practice not necessarily be hierarchically connected as shown in Figure 5-1, because local subsystems may very well be directly connected to each other, eg to meet reliability or real time requirements. From an NBO point of view, the connections form the basis for the network, and the convergence layer allows all nodes to be part of the network. The connection to *the Network* is the important issue, not the internal connectivity in the network.

The mobile subsystem will very often be connected to the local subsystem, and as such be part of that. However, mobility is handled in general terms in section 5.11. Mobility is considered an overarching issue in this work.

In the next subsections we deal with the three subsystems in more detail.

5.1.1 The local subsystem

The local subsystem covers different levels, different applications, and different technologies. An overview of the architectural views is given in Figure 5.2, where possible technologies are included. The application areas are of course examples. To the examples one might add, that the digitised soldier may carry equipment that communicates internally (ie on his body) in the form of a Personal Area Network (PAN), and externally via a Wireless LAN (WLAN). Many users will be mobile.

In our system of systems, the local subsystem is an integral part of the network. It may thus on top of the basic technologies have a convergence layer (eg IP) which will allow the nodes to expose their services to and consume services from the net.

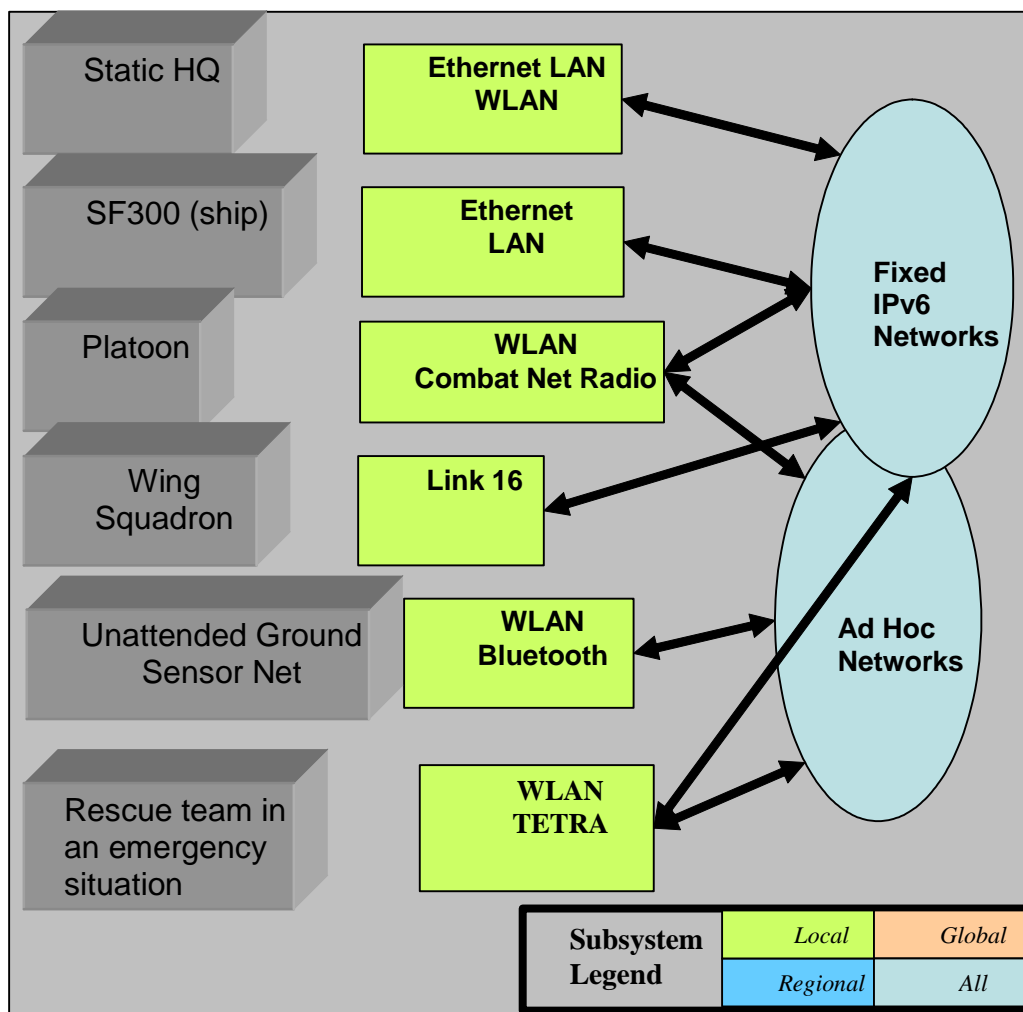


Figure 5-2: Examples of the local subsystem with possible technologies

5.1.2 The Regional and National Subsystem

The regional subsystem will typically cover an area of 50 km by 50 km. The subsystem must supply communication services to both stationary and mobile users. Examples of use of the regional subsystem are communication between land HQ components, communication between units (patrols) operating in a large area, and communications from operating units back to the HQ. The technologies will be very dependent on the actual mission parameters.

If the regional area is secured, a large number of technologies may fulfil the requirements for regional coverage. A system like DEOS is able to deliver both voice and IP-traffic. Cellular systems with transportable or mobile basis stations are another option. These systems give interoperability between military and non-military organisations, which may be of importance in management of humanitarian crises or large catastrophe situations. Both GSM/UMTS/TETRA and the new WIMAX are candidate technologies, considering requirements on transmission capacity and more specific

services. TETRA gives a possibility of detection of and reaction to jamming, while GSM is totally unprotected with regard to jamming. Regional coverage may also be obtained by use of tactical data links such as Link 16 and a number of gateways. UHF and Microwave radio relays will remain important for a foreseeable time.

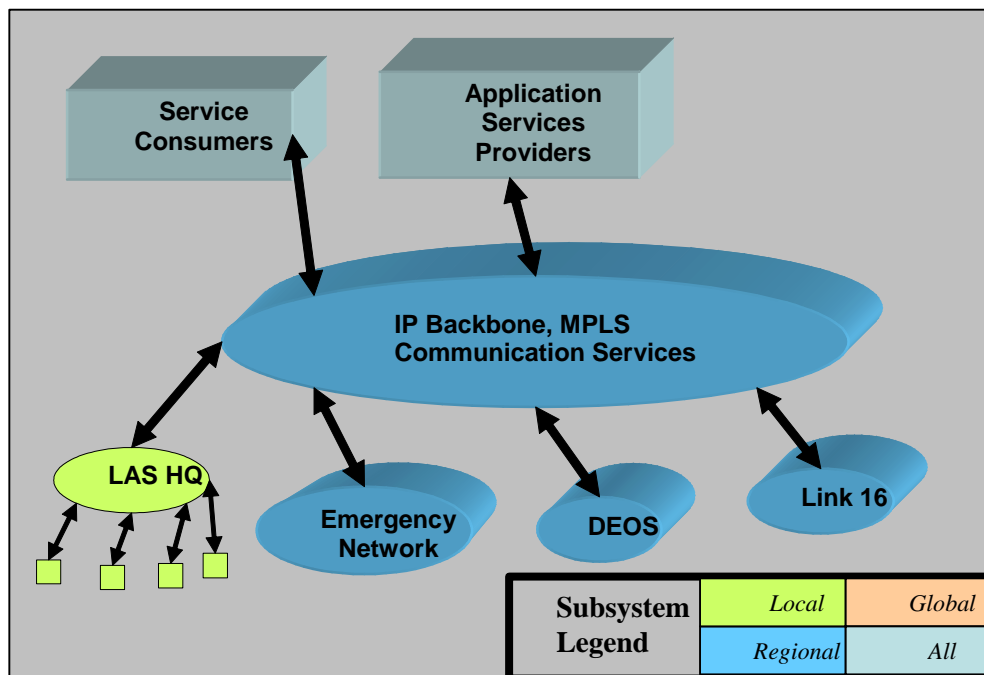


Figure 5-3: Regional subsystem with example components

An example of a regional subsystem is a communication system that covers the whole national territory or large parts of it. From an application point of view, this national subsystem may consist of a number of different interoperable communication assets, such as mobile or fixed telecommunication infrastructures, emergency networks and tactical radio systems. The convergence protocol (eg IP) and the network of networks concept glue it all together. At the application layer, SOA is a further possibility for obtaining commonality.

The relations between the LAS communication components and the regional subsystem have several implications for the performance of the total system. In principle, the local subsystems are service providers for the total system, both for applications and in this particular case the communication users. The convergence layer (eg IP) again forms the glue that makes the network of networks possible. The regional or national subsystem thus exposes a number of communication services, but these services are in many cases provided by components from the local area subsystems.

On top of the communication, a number of application services will be offered. Examples of such services are ground and air pictures, weather forecasts, information on the road traffic situation, regional directory services, and commander's intent. The regional subsystem is an important contributor to common situation awareness for all actors in the region.

It is important to note, that SOA allows a weak coupling between the contributing subsystems, so that they may evolve at their pace as long as they play by the rules of the communication infrastructure, ie they are and stay *net-worthy*.

5.1.3 The Global Subsystem

The global communication subsystem has the task of providing communications over long distances. Figure 5-4 illustrates that the systems contributing to global communication subsystem are either tunnels for the IP-traffic or genuine IP-providers.

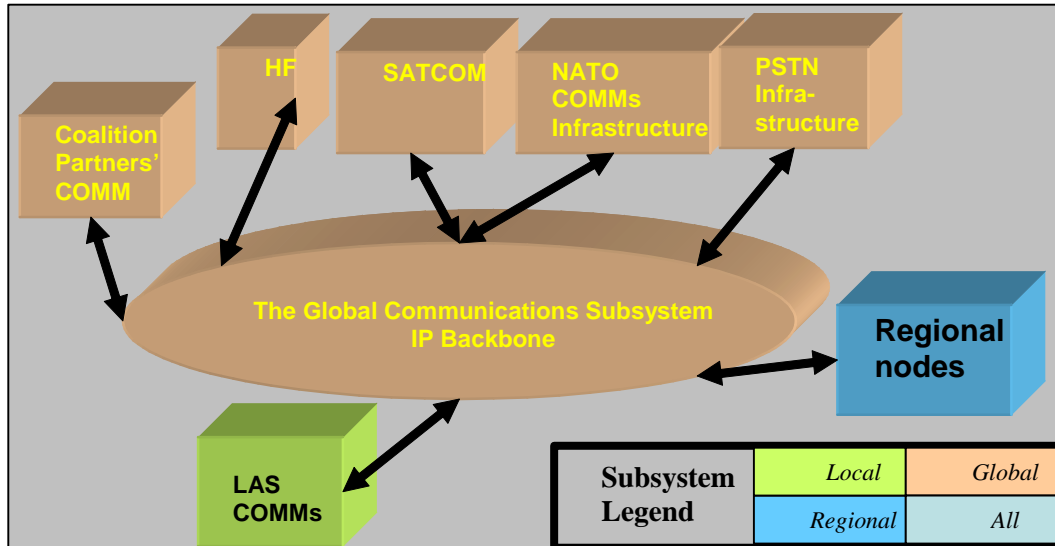


Figure 5-4: Global Communication Subsystem with IP-tunnels or IP-providers.

The most relevant technologies are HF radio and satellite communications (SATCOM). Communications back to the national strategic level from units deployed far away from Denmark is the most important task of the global subsystem [Ref.1]. The system must be capable of delivering so rich information that the situation picture and a common situational awareness can be created and maintained across the vast distances. There are few real time requirements, so that even very small transmission capacities may give a useful contribution. The global subsystem will also be an important link between the deployed units and the national logistics organisation.

Requirements on availability of this subsystem are high, so it is important to offer redundant connectivity where different basic technologies are used.

On top of the communication subsystem, a number of service providers and service consumers will reside.

5.1.4 Concluding Remarks on Subsystems

This architectural view gives a partition of the communication infrastructure in a logical hierarchy, where coverage of geographical area is the governing principle. The technology used in the subsystems is to some degree specific for each of them, and their peculiarities are directly traceable to different operational requirements. From an NBO point of view, the partition into three communications subsystems will not clash against the vision of a global information grid. The loose coupling and the convergence (eg the IP-suite) will allow the contributing subsystems to evolve at their own pace.

5.2 IP-Convergence

The purpose of this architectural view is to establish the IP-suite as the main vehicle for communication interoperability, ie as the protocol that allows routing and addressing in the network of networks. By using the IP-suite to integrate all nets, a number of advantages can be achieved such as platform and operating system independence, easy integration with a large number of transport and application protocols, and access to many commercially available gateways to dedicated military nets.

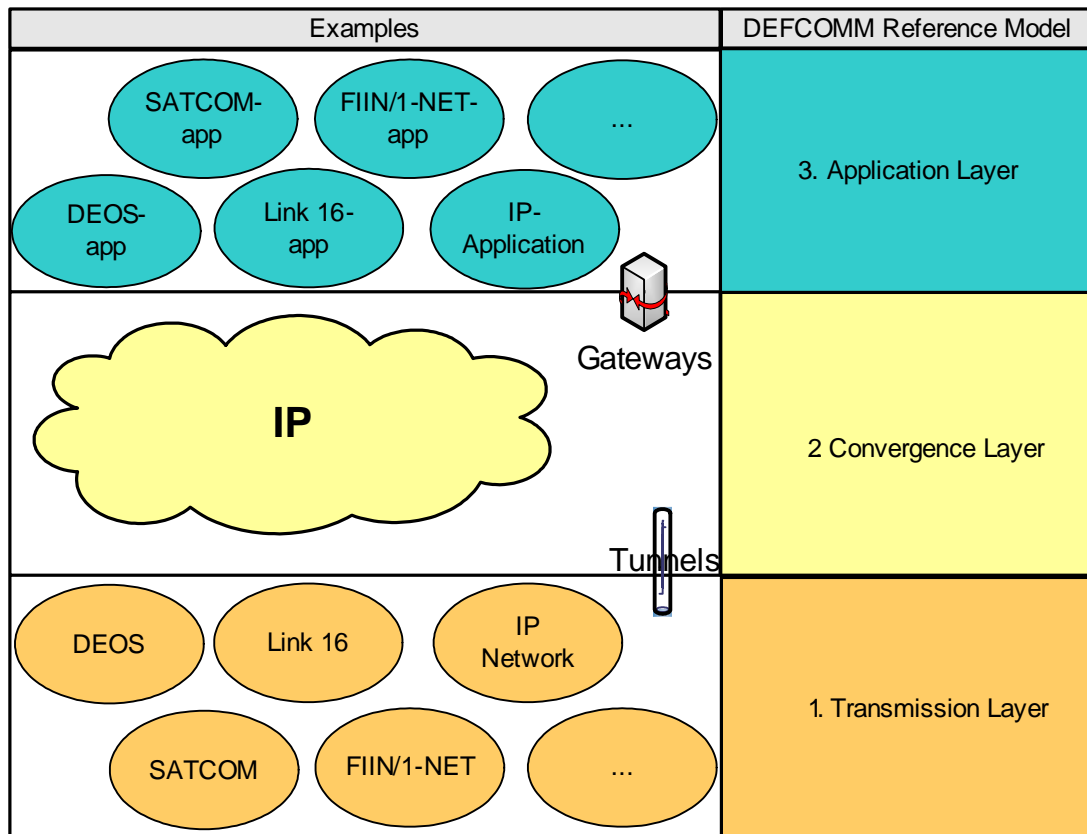


Figure 5-5: IP-convergence layer interworking with other networks/applications

The use of the IP as the convergence protocol is shown in Figure 5-5 above where the possible relations with other networks are shown. The gateways are used for communication between non-IP applications and the IP-convergence layer is, while tunnels are used IP-communication through other networks. It is a matter of choice, how much the IP-addressing will be used in the dedicated networks, at least in the initial phase.

The advantages of using IP as the overarching protocol are many. Most important is its wide use and acceptance, which means that most vendors either use it as a native network protocol or support it, so that interfaces to the IP-network are easy and relatively cheap to establish. The interface may be gateways or tunnel solutions. The dominating position of the IP (including IPv6) will last for the next 15 years. The IP (both IPv4 and IPv6) is a connectionless protocol, a best-effort protocol. The IP thus does not guarantee that its protocol data units, the packets, arrive at their destination. Damaged packets are discarded. Error control such as retransmissions must be

done by other protocol layers, such as the transport layer protocol TCP. The IP has other limitations such as a very limited range of Quality of Service (QoS) parameters. There is a lack of real-time performance. This means that for a number of communication tasks, the IP will be insufficient, and more dedicated networks such as tactical datalinks (TDLs) must be used also in the future for a long period of time. The IP has otherwise proven itself to be a robust and versatile protocol.

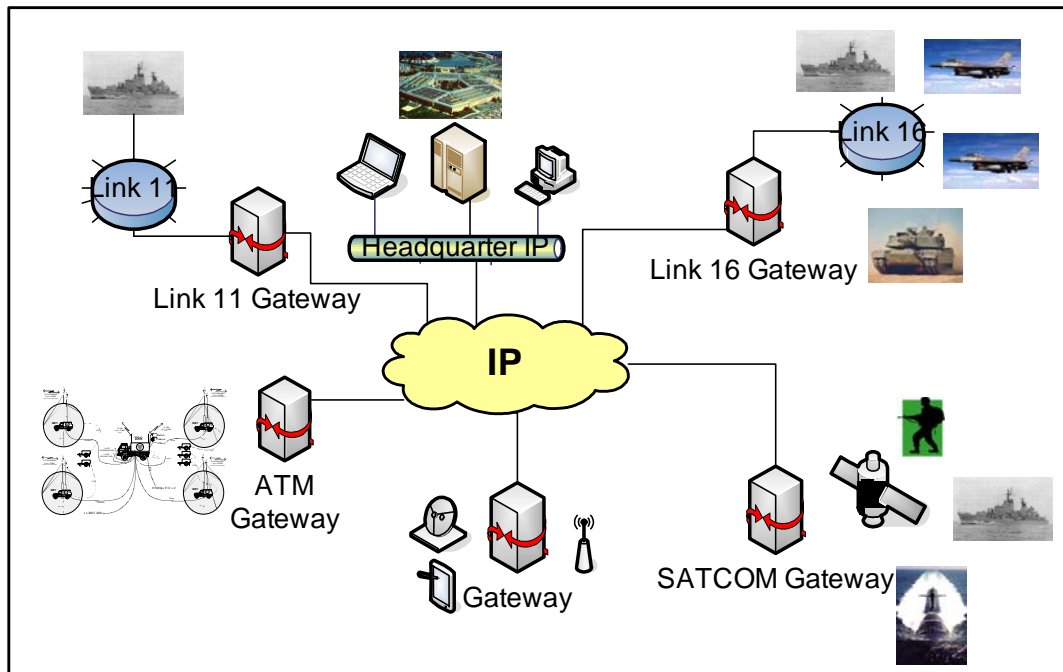


Figure 5-6: IP-network of networks - Gateways used for connectivity to other networks

It is also possible to consider the total networks of networks in another way. The figure above shows that the network of networks consists of dedicated networks, and networks that use the IP as their native protocol. In some cases end-to-end communication is achieved by use of gateways and different access networks, in other cases the communication devices use only the IP.

Figure 5-7 shows the convergence layer view in another perspective. The gateways are dual home devices and perform the necessary translation between the native protocols and the IP-suite in the global net.

In Figure 5-8 the link 16 network may be a service provider so that in this case it delivers a sensor image to a ground based workstation. The real-time properties (guarantee) of the link 16 communication will not be preserved in this data exchange.

5.2.1 Gateways

The initial reference is Figure 5-6. In the middle of the figure an IP-network is shown. The network is connected to subsystems in the ie other networks and tactical data links, not based on IP. The IP-network forms the infrastructure which in principle

connects to all networks and tactical data links through gateways. Separate IP-networks can be connected to the IP-infrastructure without the use of gateways.

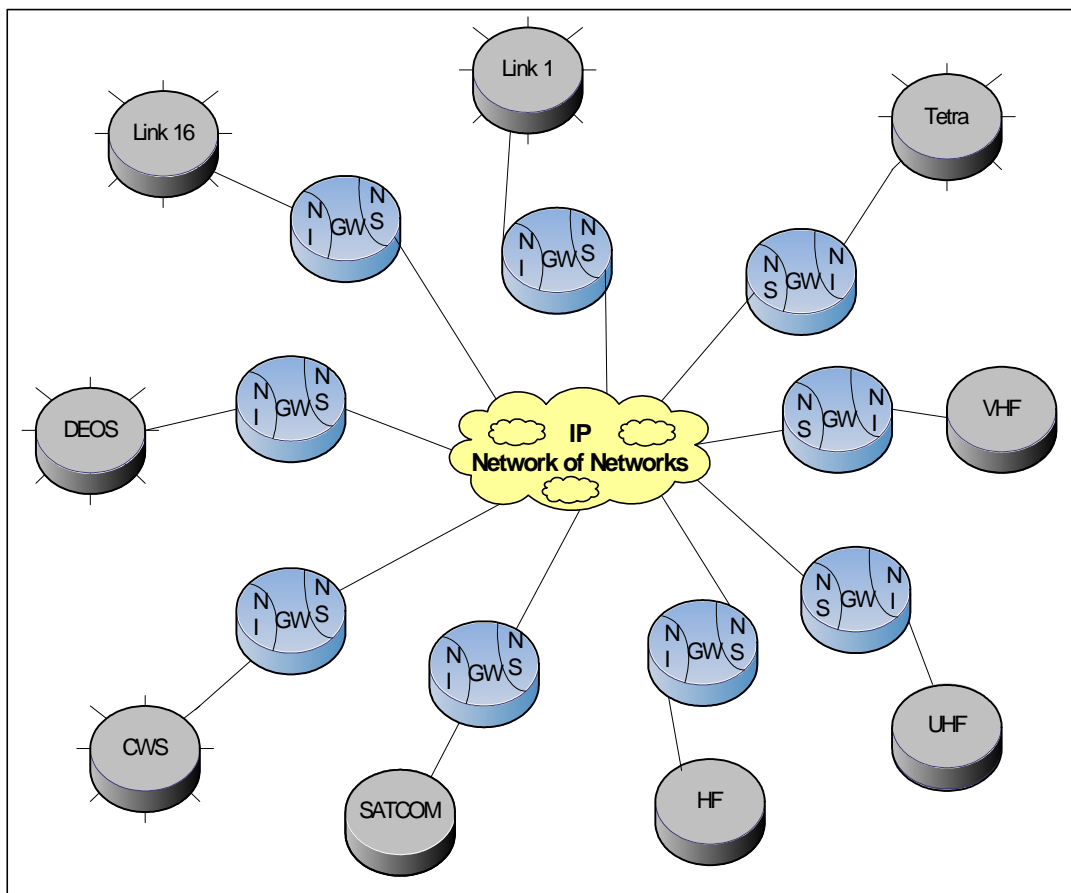


Figure 5-7: The IP-convergence architectural view

This architecture makes it possible for all data to be accessed at any position in the network. In practice the data that can be accessed depends on:

- Gateway functionality
- Subsystem functionality
- Limitations due to security (eg confidentiality)

The best opportunities for data access are on the IP-infrastructure. It is in principle possible to view a situation picture from eg Link 16 through a gateway or hear/transmit voice etc.

A user connected to one of the subsystems will be able to receive data from the IP-network as well as from other subsystems. The requirements are that the gateway functionality is present and that the subsystem including terminals supports the data. For example a Link 16 user will be able to communicate to headquarters with the use of voice but will not be able to see the contents of a database.

The native properties of the networks or tactical data links are not necessarily preserved. For instance the Link 16 real time and confidentiality properties will not be preserved outside the Link 16 network. If these properties are to be preserved they

must be implemented in the IP-infrastructure, which may implicate that one may wait for an evolution of the IP-suite.

A gateway (Figure 5-7) logically contains a Network Services (NS) part which offers services to the IP-network and a Network Interface (NI) part which connects to the native network, tactical data link or radio. In the case of a gateway for Link 16 the NI could be a MIDS terminal. Between NS and NI an interface for data conversion, communication, buffering, address converting etc is placed.

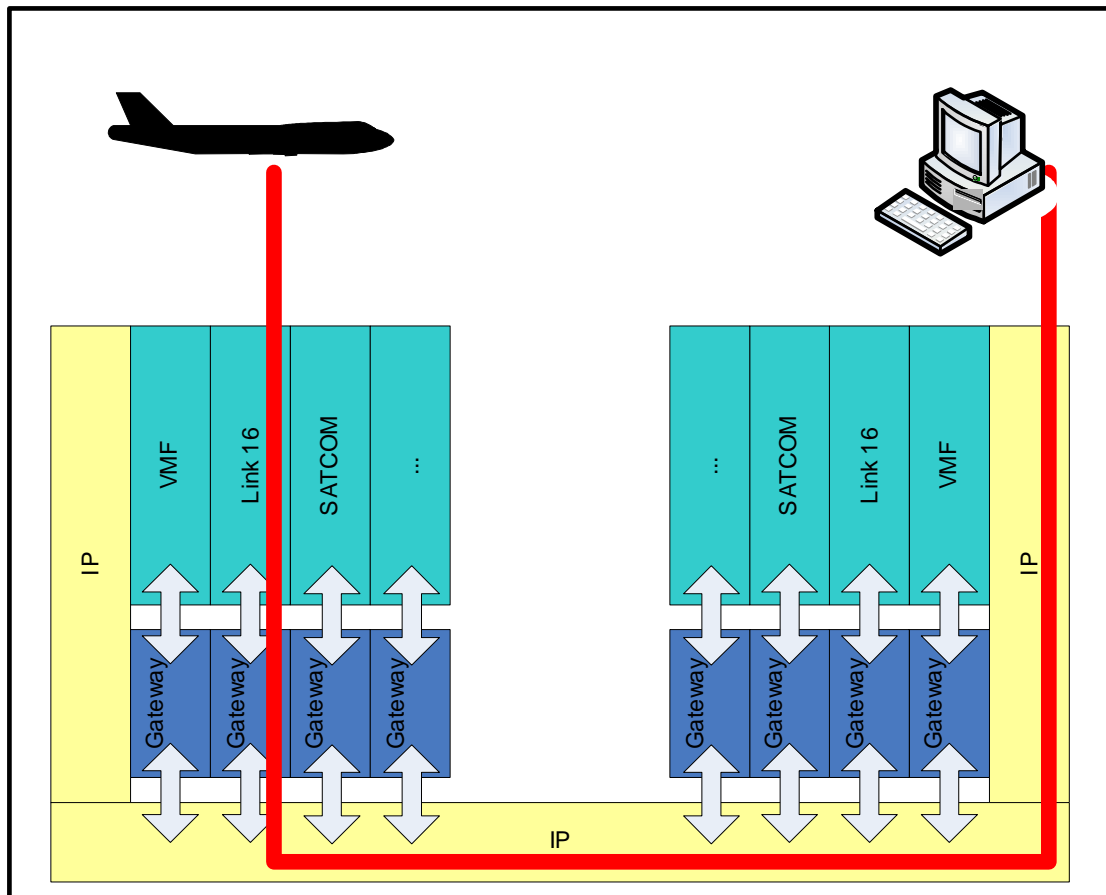


Figure 5-8: Example of gateway based data exchange between different devices

In Figure 5-8 an example of data communication between a PC and the Link 16 network is shown. Link 16 provides eg the situation picture for the IP-network via the connected gateway. A Link 16 to IP gateway is a requirement.

Some gateways might be acquired as COTS or dedicated systems, and research and development in this area are expected in the years to come.

5.2.2 IP-tunnel

At the transmission layer (ie below the convergence layer) several transmission technologies can come into play. As indicated on Figure 5-9, wired connections such as Ethernet or Asynchronous Transmission Method (ATM), wireless connections

such as IEEE-802.11 or 802.16 or dedicated connections such as tactical data links such as Link 16 or DEOS can all be used to carry IP-traffic.

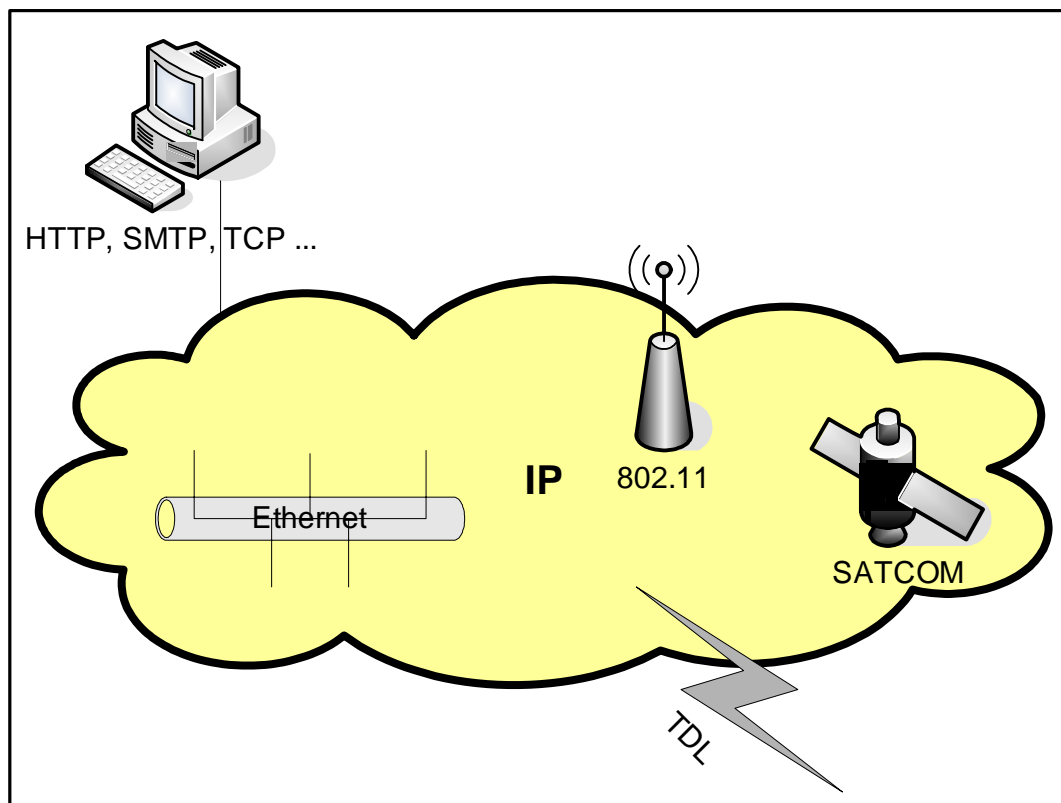


Figure 5-9: Integration of different transmission mechanisms

Tunnelling or gateways can be used, if the technology at hand does not directly support IP-traffic. For example two gateways allow IP traffic to be tunneled through Link 16. Figure 5-10 indicates a situation where two physically separated IP-nets are connected logically in this way. Each IP-network communicates with a Link-16 terminal through a gateway. On transmission, the gateway supplies the necessary headers to include the IP-messages in Link-16 packages. Similarly, the gateway connected to the receiving Link-16 terminal can reconstruct the original IP-messages from the Link-16 packages received.

5.2.3 VHF-example

For a more detailed example consider a gateway between IP and VHF radio.

The gateway is through a router connected to the IP-net as a Network Service (NS) and to the VHF radio as a Network Interface (NI). Here NS is a Voice over IP (VoIP) channel, offering the service of voice transmission to IP-users. NS is a VHF radio whose output lines for speaker, microphone and switching are connected through the actual gateway to the VoIP device (Figure 5-10).

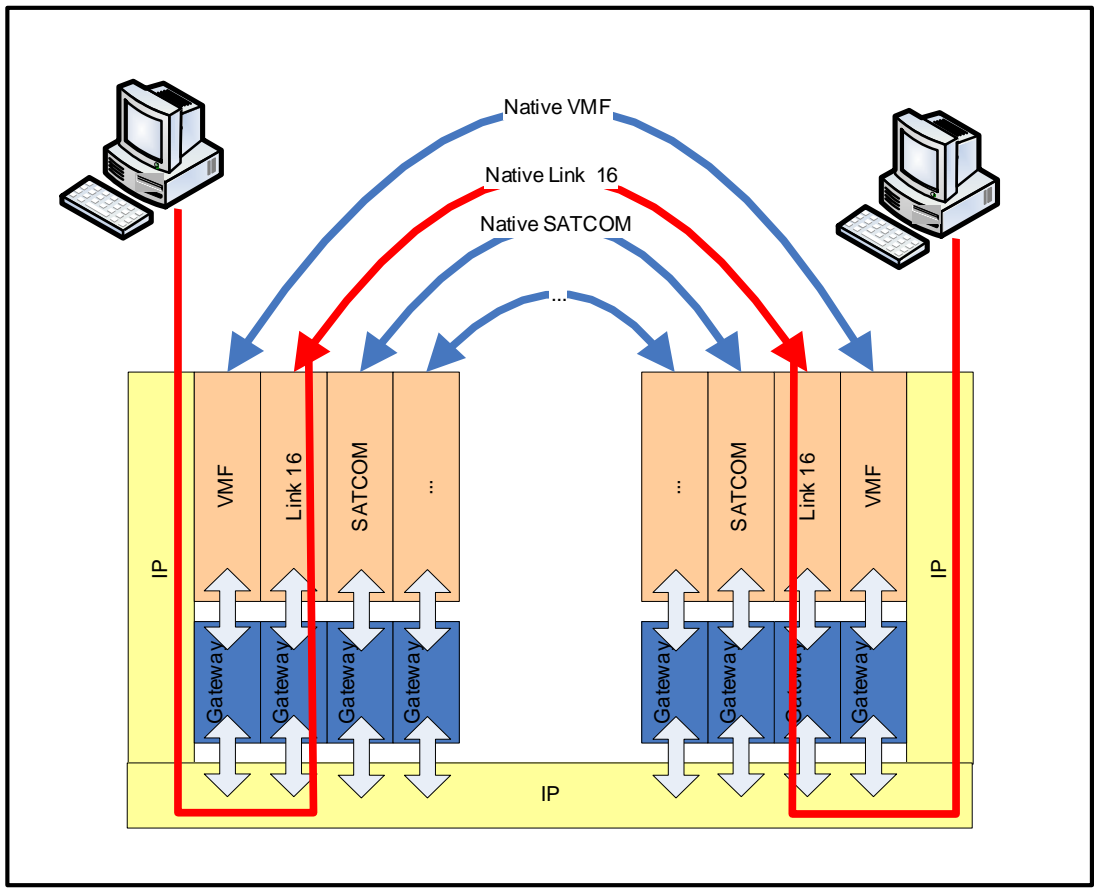


Figure 5-10: Tunnelling of IP-traffic through Link16 TDL

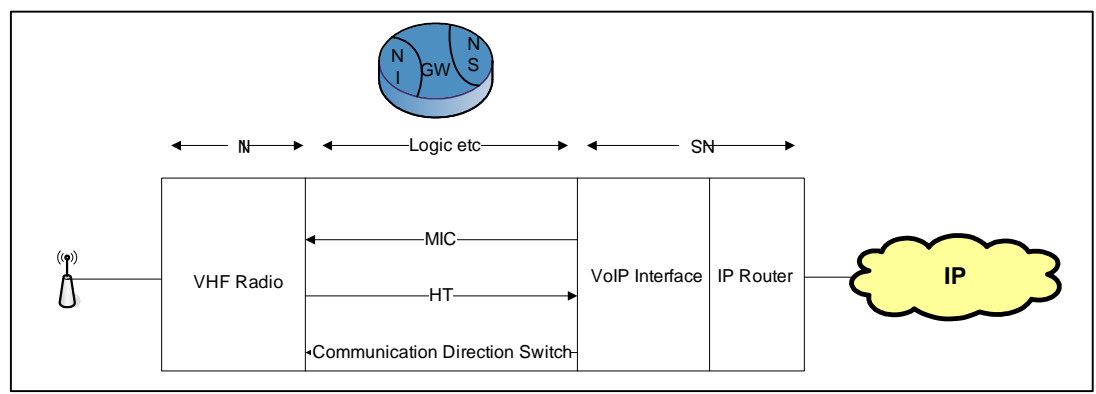


Figure 5-11: VHF Example – Gateway for VoIP

Note that Voice over IP-devices are widely available as COTS. Also the complete package including NS, Gateway and NI is commercially available³.

³ The modem IDM V304 is an example. This modem uses military communication standards for transmission of IP traffic over VHF, thus providing access to IP data in military vehicles. Possible uses include situational awareness, blue force tracking, positioning, target selection. Technically IDM V304 is a 6-channel RF-IP converter. Transmission capability is 16kb/sec.

As indicated on Figure 5-12, tunnelling requires the use of two gateways. We see that tunnelling allows transmission of data between users or systems from separate IP networks.

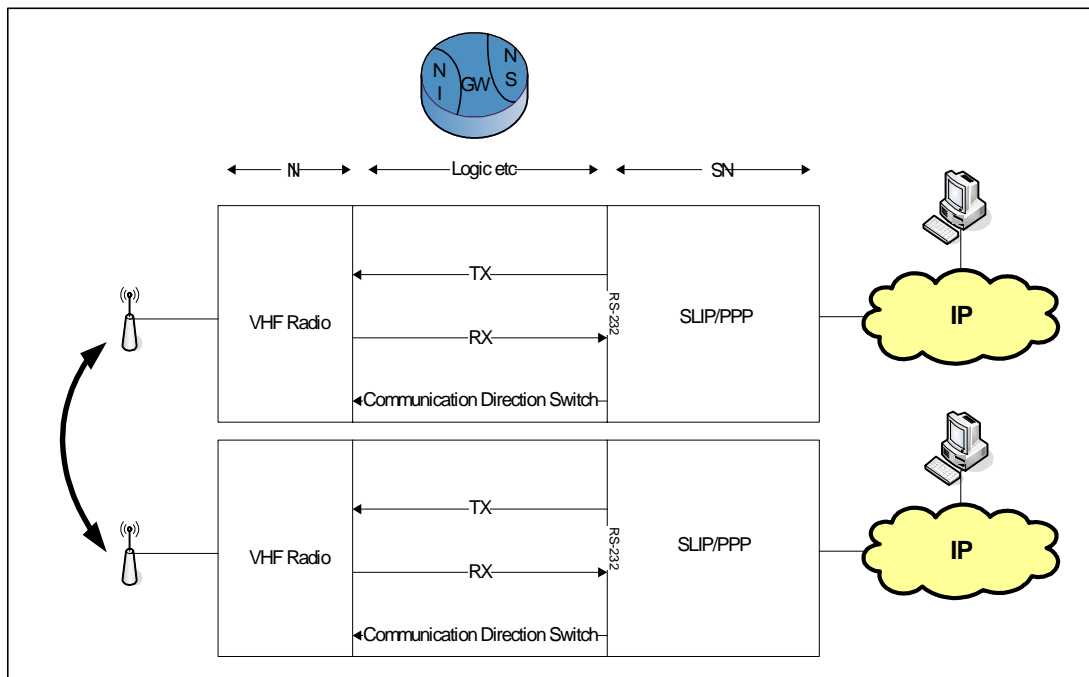


Figure 5-12: VHF Example - Tunnel of IP-traffic through VHF radio

5.2.4 Concluding remarks on IP-convergence

This architectural view is based upon a networked infrastructure, where the IP-suite is being used as a converging protocol for all types of communication, whether voice, video, or data. Use of gateways will allow access to other types of networks such as TDLs.

The IP-infrastructure can be built from standard commercial IP-components, using tunnelling through the transmission mechanisms at layer 1 of the communicating model. The same IP-tunnelling will also allow TDLs to be used as a vehicle for transmission.

This architectural view will allow global access to all data. The IP-suite will provide the basis for relevant applications such as VoIP or Mail, and protocols such as HTTP, SOAP etc. Other and autonomous networks may co-exist. Gateways will allow exchange of data or services between the nets, the actual gateways will determine to which extent. However, note that in general not all original properties of the information exchanged may be preserved. For example a current-technology IP-network cannot uphold the real-time property of TDL communication.

5.3 A Global Information Network

The purpose of this section is to describe a global information network, which will allow transmission of data between geographically disparate locations, eg from headquarters in Denmark to camp in Iraq, from camp to expeditionary group, from the group to the individual soldier. Establishing a connection will be transparent. The user will select the service to use, eg voice, video, text. After that, the global information network will automatically select the most appropriate communication path for the transmission.

The global information grid will of necessity consist of many different communication technologies – for examples see Figure 5-13 below. When a connection is to be established, the technology will be chosen according to required parameters, such as range, transmission capacity, size, weight, security, cost etc. In case of joint or combined operations, the range of communication technologies of all participants must be considered. The objective is integration of all technologies at hand. Potentially, all users should have access to all networks and any information, according to need and classification. All connections should be seamless, plug-and-play.

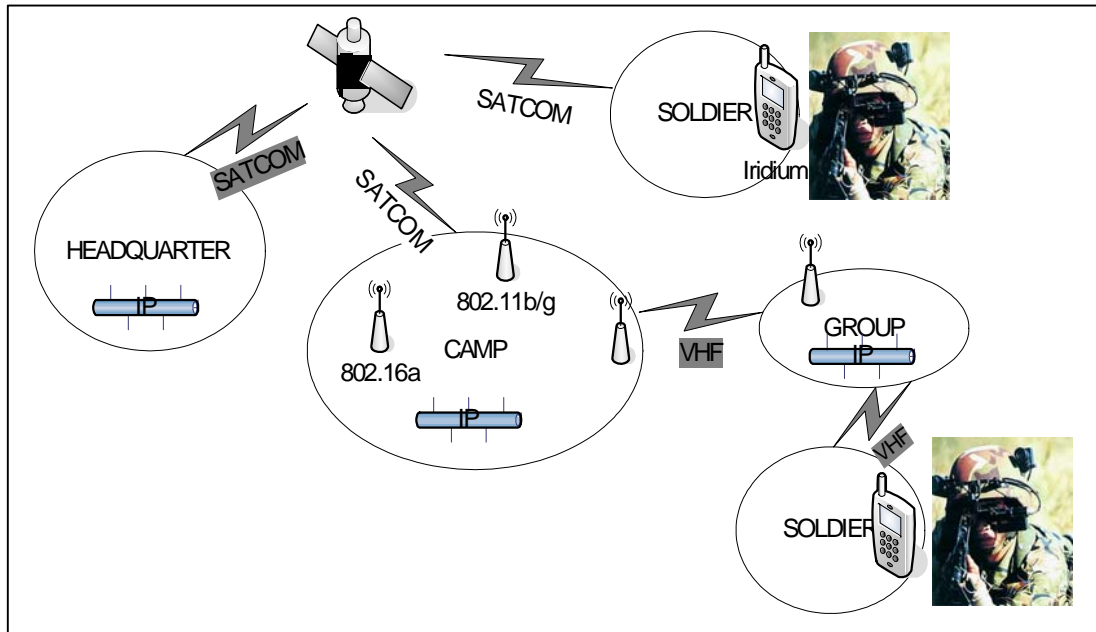


Figure 5-13: Examples of communication technologies in a global information network

Use of tunnelling will allow IP-based data communication over technologies without inherent IP-capability, as outlined in section 5.2. For example, VHF radio can be used as carrier for IP-traffic.

The global information network implies that transmission of IP-packages is globally feasible. The terminal and network connections at hand will determine what services can be used. For example, a voice connection from force headquarters to the soldier in the field, may utilize a combination of ordinary telephone lines, voice over IP, and VHF radio. When equipped with the proper sensors and display, the future soldier will be able to send and receive voice, images, video and text.

5.3.1 Transmission layer communication

Organisation and deployment of military units provide a natural grouping of transmission layer communication architecture. The following grouping of military communications arises from geographical distances and the military organisation in general (see also [Ref.1] and [Ref. 2]).

- Personal communication. PAN, Personal Area Network. The individual soldier may be equipped with devices (eg microphone, PDA, sensors, etc) which may communicate internally with each other, or externally with other members of the same group or section. Connections may be wired or wireless. Bluetooth, IEEE 802.15.x, either high-speed or low-speed may be of use here..
- Group/section communication. Mobile communication within a limited area. In general high transmission capacity, although occasionally buildings or other structures in the fighting area may result in limited transmission capacity. Need for tight integration person-to-person and person-to-sensor. Need for real-time transmission of target data or identifications in the form of video, images or voice. (At this level we presently find VHF communication)
- Inter-unit communication. Here we have at the same time a demand for mobility and the need to cover a large area. In consequence wired communications are not practical, and Line-of-sight cannot be assumed. At this level, the communication needs are very diverse, such as information systems update (including transactions), or transfer of images, target data, identifications, or voice communication. Fortunately demand for real-time communication tends to be less important here than in group/section communication. [at this level we presently find HF, VHF, and UHF communication]
- Strategic Communication. Here the distances involved are so large, that only HF, SATCOM or permanent wired lines can be used. Real-time communication is not important. Communication needs cover information systems update, supporting systems, images and voice. In general, some delay may be accepted, since in any case the decisions to be taken involve long-ranging factors. [At this level we presently find HF and SATCOM]
- Communication within command installations. Here the need for communication covers information systems update, office automation and voice. The distances involved allow the use of wired communication lines or short-range wireless connections throughout. [At this level we presently find wire-based phones and commercial LAN]
- Support communication. Includes communication that is established independently of the organisational hierarchy, such as fire support or air support communication. Characterized by hard real-time requirements, fairly high distances, and fairly high transmission capacity. Support communication will be established ad hoc, but it is essential that it can be established at any given time. Queuing is not acceptable. [At this level we presently find Link systems, VHF and HF communication]

Ideally, this division should be abolished. It would be desirable to have a single large net, using homogeneous transmission layer, but this ideal is presently unattainable. Using present technology, such a homogeneous net would be restricted by the

physical relations between frequency, distance, and transmission capacity. In order to obtain communication over large distances, a severe limit on bandwidth must be accepted. Hence such a system would be unable to satisfy the communication needs of all levels at the same time.

However, modern use of satellites or airborne communication junctions may go a long way towards achieving such a homogeneous net encompassing all military levels. An example is the US system "Blue Force Tracker"

Another possibility is to use multi-band SDR (Software Defined Radio) which effectively removes the borders between HF, VHF and UHF communication. In theory such a system could adapt any communication at hand to use the frequency resulting in maximum transmission capacity.

In theory a visionary target communication architecture having a single transmission layer medium is possible, based upon either SATCOM or SDR.

Within the time horizon of the present report we estimate that Denmark must continue to use heterogeneous architecture at the physical level. We conclude that transmission layer target architecture at least for the time being must continue to support several communication types, due to the physical relations between frequency, distance, and transmission capacity.

5.3.2 NBO aspects

The global communication network allows for communication in all directions in the otherwise hierarchical military organization. In principle everyone may communicate with everyone, giving all information immense logical reach. The important thing is having mechanisms ensuring proper prioritisation of the information, and enforcing demands for confidence, need-to-know, or need-to-share.

5.3.3 Concluding remarks on the global information network

The global information network allows communication from everyone to everyone in the network, irrespective of geographical or hierarchical position. The communicator may be a human user, a process, a terminal or a computer host.

Interoperability at the layer of convergence must be supplemented by flexible transport mechanisms which can be selected and combined according to the communication needs at hand, such as transmission capacity, geographical distances or security.

Operational needs may call for different transmission media for different types of communications as listed above. (Personal, Group/section, Inter-unit, Strategic, Headquarters) The global information network will integrate all transmission media using a common convergence protocol, such as IP, either in the form of native components or using gateways or tunnel solutions through otherwise incompatible networked infrastructures.

5.4 Quality of service (QoS)

This section describes an architectural view where Quality of Service mechanisms are an integral part of all networking components. The aim is to optimally allocate all network resources in order to satisfy QoS demands from the network users⁴

In order to discuss QoS and resource reservation in general, we introduce an architecture that will allow the user to specify end-to-end QoS in a heterogeneous communication infrastructure. The architecture must support various services and applications on a variety of network components. To achieve this, we dynamically add QoS-components to the network according to the demand at hand [Ref. 2].

Regarding the reference model used in this work, QoS must be considered at all three layers. Here, however, we will focus on QoS components at the Convergence layer, which are to ensure a uniform QoS even if the underlying transmission layer consists of heterogeneous transport mechanisms. In this way, the overlying service layer may assume the existence of homogeneous QoS components.

5.4.1 Background

During recent years, network development in general has given us ever increasing bandwidth, resulting in correspondingly better ability to accommodate demands for QoS. At the same time, however, an increasing number of services and applications demand specific QoS levels regarding network accessibility and temporal predictability. In principle, the networked infrastructure must be able to support every demand, ranging from real-time embedded control systems to best-effort systems, such as www-applications. The communication infrastructure must include QoS components to allow an application to specify its demands in this respect.

In order to affect a QoS communication infrastructure, QoS resources must be supplied from the transmission layer. At the same time, differing networked infrastructures and differing network protocols must be able to coexist at this layer. Also differing reservation mechanisms must be allowed to coexist in a network of networks. Ideally, any application may be allowed to specify its demand for QoS using the functions of the convergence layer, irrespective of the actual technology used in the underlying layer.

5.4.2 Introduction

QoS refers to the ability of a net to guarantee transmission predictability for network services, irrespective of the underlying network technologies, such as Frame Relay, ATM, IP, SHD/SONET, Ethernet, wireless, etc, - either singly or in combination.

The International Telecommunications Union (ITU-T) gives the following broad definition of QoS:

⁴ Throughout this report the term "user" is used in a broad sense, meaning any network user, whether human, terminal, application, process, PDA, sensor, etc.

"The collective effect of service performances, which determine the degree of satisfaction of a user of the service"

According to this definition, the notion of QoS describes a combination of qualitative and quantitative concepts. Quantitative concepts are directly measurable characteristics, specific to the service under consideration. Examples are bandwidth, delay, jitter, Service Level Agreement (SLA), etc. Qualitative concepts include the notion of user satisfaction, ie the extent to which users' need for data communication is satisfied.

5.4.3 End-to-End QoS

The service level of a network is defined as a measure for its ability to deliver end-to-end⁵ (E2E) communication with a specific degree of QoS. In this perspective, the most important difference from one transport service to another is their respective degree of QoS. In other words, their ability to guarantee specific levels of specific properties such as bandwidth, delay, jitter, loss-characteristics, etc.

Our target architecture for military communication will focus on QoS as seen from the convergence layer. Control and management of QoS parameters will take place at this layer. QoS at the application layer is a function of the individual applications, rather than the network itself.

At the convergence layer, we have the following 3 classes of QoS over a heterogeneous network

- Best effort services, ie information are transmitted, when and if possible. Indefinite delay may occur. Best effort services are the epitome of IP and the Internet.
- Differentiated services; some traffic is more important than other and is given priority. Differentiated service is useful, when a network must carry traffic from widely different applications, such as network management, alarms, high priority information and office applications.
- Guaranteed services Useful when proper functioning of specific applications, typically due to hard real-time demands, needs guaranteed levels of some network resources, such as bandwidth, delay, jitter or package loss.

5.4.4 Resource allocation

Resource allocation implies that parts of the communication system are reserved for specific entities. The mechanism of reservation must be able to deal intelligently with a situation where any number of users at any time is competing for a limited quantity of network resources. According to the operational situation, this mechanism must decide whether the resources at hand are sufficient, or whether additional resources are called for.

⁵ Note that when used in connection with QoS, the acronym E2E has actually two slightly differing meanings: either end-to-end, meaning user-to-user, or edge-to-edge, meaning from one side of a network to the other. In any case, the difference is very subtle.

Protocols for resource reservations are an important factor if network applications are to obtain satisfactory QoS. Usually they reside at the lowest levels of the reference model.

Several mechanisms of reservations are implemented at various places in our reference model to guarantee that specific applications can have network resources at their disposal. Asynchronous Transfer Method (ATM) is an efficient protocol functioning at the borderline between transport layer and convergence layer. Resource Reservation Protocol (RSVP) resides inside the convergence layer. Real Time Protocol (RTP) exemplifies a protocol used at the borderline between convergence layer and application layer.

5.4.5 QoS architecture

The QoS architecture must reflect the integration of QoS mechanisms throughout the network system, and provide for QoS transparency through all layers of the communication model. According to user needs, the QoS architecture must support dynamic resource reallocation.

5.4.6 Heterogeneous networks

It is paramount for the architecture to support an open, distributed and heterogeneous environment. This implies that the coexistence of several protocols and different sorts of hardware must be supported. Also, the architecture must support all the different application types, which may request QoS irrespective of the transmission mechanisms being used.

The QoS architecture must be portable to other network platforms. If a mechanism at the transport layer is changed, or even disappears, the ability of the architecture to manage QoS must be maintained. Insertion of new application protocols must be possible at all times. All this calls for a very modular and component-oriented architecture.

QoS components at the convergence layer are:

- **Service Level Agreement (SLA).** The purpose of SLA is to ensure a proper mapping of QoS specifications from one level of abstraction to another. For example, at the application level the quality of a video transmission may require a certain number of frames per second. Too few frames result in unacceptable quality, ie flickering or drop outs. However, the lower layers do not have the notion of frames. Here the desired level of QoS must be requested in units such as bandwidth or processing speed. In a converged heterogeneous networked infrastructure such mappings are absolutely essential to secure a desired level of QoS. In principle the user does not know, and indeed does not need to know, anything about which components of the net, his traffic is passing through. Using SLA, the originally specified QoS will transit the entire network, expressed as parameters that are meaningful locally.
- **Signalling.** Deliverance of end-to-end QoS requires that every network element in the actual communication line (switch, router, firewall, host, client, etc) respects the required QoS. Coordination calls for a QoS signalling protocol, ideally functioning end-to-end over the heterogeneous networked infra-

structure. Unfortunately, all present signalling protocols have some limitations in this respect.

- **QoS policy.** QoS policy includes management and accounting, etc. At least the following QoS policy functions must be included:
 - Authentication of users (end-users, hosts, applications, etc.)
 - Authorization of users to use the different network services
 - Access control, based on factors such as user, application, priority, time, bandwidth, etc
 - Accounting, keeping track of usage of all network resources, service level, domains, etc
 - Congestion management
 - Routing
 - Link optimisation

Figure 5-14 indicates placement of these QoS components in the target architecture. See also chapter 3, where the QoS components are discussed in relation to the DEFCOMM reference model.

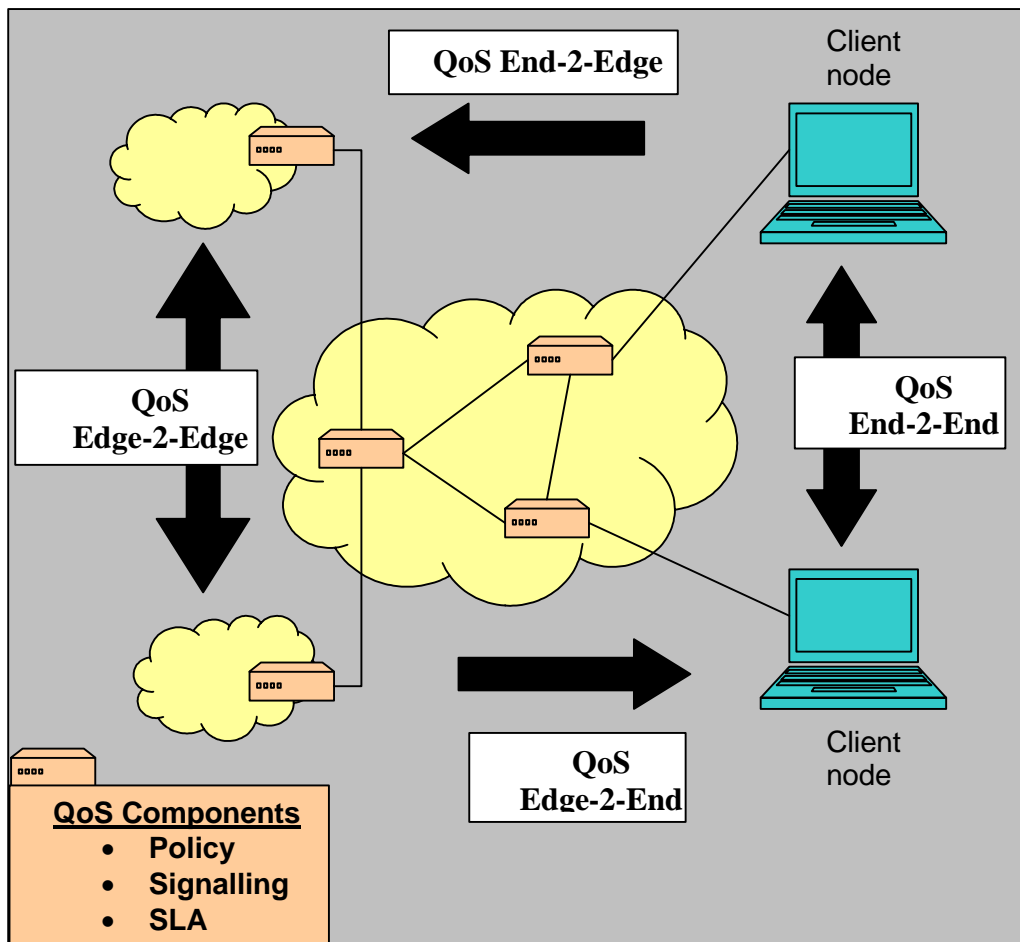


Figure 5-14: Main components of QoS at the Convergence layer

5.4.7 Concluding remarks on QoS

The objective of this architectural view is to give applications and processes at the application layer a transparent view of QoS. The actual reservation protocols and other mechanisms used at the lower layer to deliver the requested QoS are hidden from the requester. Hence any existing transmission mechanism having QoS abilities can be included in this view, and any new mechanisms may be added. Also, the architectural view is scalable regarding support for new applications and new reservation protocols. When desired such components can be modified or new added.

5.5 Security

The purpose of the security architectural view is to identify the components which will ensure the security of the Danish Armed Forces target architecture, ie availability, confidentiality, integrity, authenticity and non-repudiation. The security architectural view is in this context limited to a framework for components to be used in other architectural views. The security architectural view is closely connected to these other architectural views.

Besides the technical requirements extracted from WP2, regulations from the Danish Armed Forces (eg FKO-358-1) also have to be obeyed. The security architectural view must comply with directives and technology as known today and at the same time taking prospects for future NBO requirements into account.

The necessary security must be incorporated in the target architecture, also in cases where scalable solutions are unknown today. This is one reason for only including generic components in the security architectural view.

The security risks relevant for the security architectural view include:

- Unauthorized users getting access to network
- External attacks, both physical attacks (eg from adverse weather or by weapons) and logical attacks (eg denial of service)
- Internal threats where authorized personnel causes damage or degradation of network resources
- Vulnerability in hardware or software especially when using COTS
- Configuration errors in network or applications

The security architectural view is of relevance to all layers in the communication model. However, different types of security considerations may apply at each layer. In general, security of the target architecture is determined by the following five architectural views:

- Availability
- Management of cryptographic methods
- Confidentiality, - including security domains and enclaves
- Access control, - both locally and globally
- NBO security aspects

5.5.1 Availability

The purpose of the availability architectural view is to make sure that the information can be accessed in daily work, be available for missions with high communication intensity, and for mission critical communication. As a principle, full availability is required; however, a degraded capacity can be accepted under certain circumstances eg depending on the communication intensity.

The overall principles are defence-in-depth of the ICT Systems, and boundary protection. The requirement is an architecture without any single-point-of-failure and consisting of robust and failsafe systems. Availability must be present at all layers in the DEFCOMM reference model. If availability is missing at a lower layer it can not be present at a higher layer.

In the availability architectural view the availability can be ensured by the following requirements:

1. Redundant transmission mechanisms at the transmission layer, eg alternative media and/or networks. Redundancy at the transmission layer will allow higher level protocols the choice between alternative media or networks
2. Robust transmission mechanisms, eg jamming-resistant media
3. Management agents able to monitor and control the resources of the network in such a way that limited resources are used in an effective manner. The communication to and from these agents must have priority.
4. Detection of and recovery from intrusions. This includes boundary protection, Intrusion Detection Systems (IDS), anti-virus systems, and recovery functionality.
5. Partitioning of the network into logical or physical security domains to prevent the spread of degradation from one part on the network to another. The domains can be separated by firewalls, filters, etc.

Requirements 1 and 2 are satisfied immediately when relevant convergence protocols are used. The key requirement is that the actual transmission mechanism has an effective interface to the protocol in use eg the IP-suite.

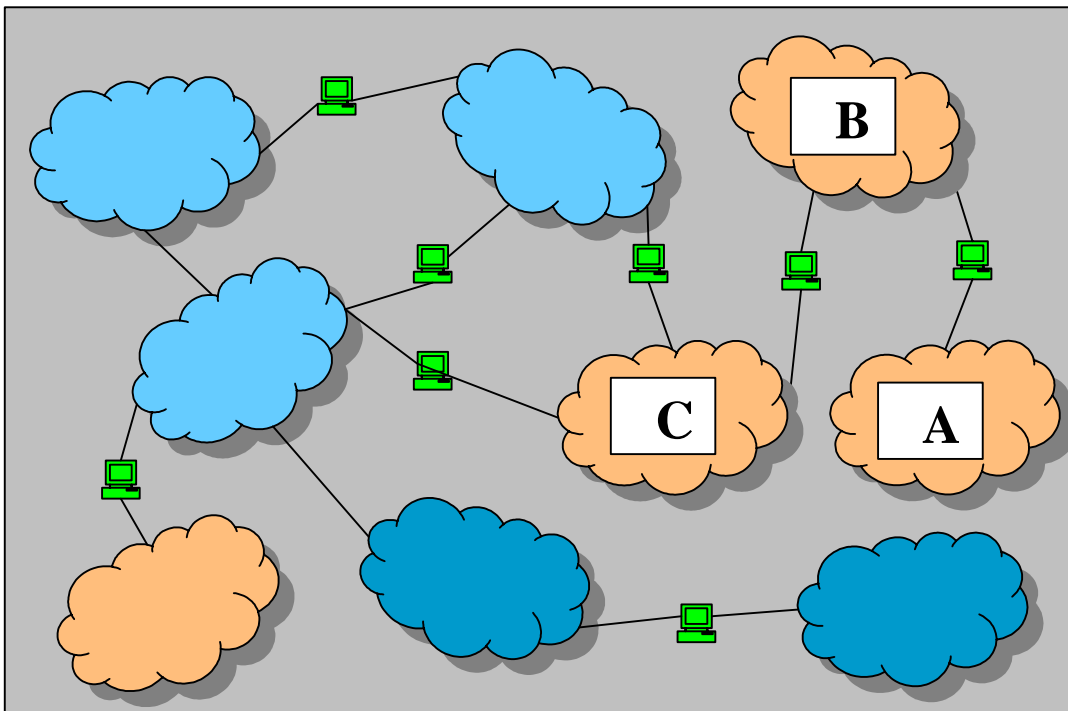


Figure 5-15: Example of domain partition in order to control availability

Requirement 3 is to be discussed in the Network Management section. Since networks based on the IP-suite are vulnerable to denial of service attack, it might be necessary to have alternative routing of management information. In that way a central part of the network can be controlled out-of-band by separate networks, channels, or by manual intervention.

Requirement 4 implies that information about attack is communicated to other parts of the network. This may also call for alternative routing in case the primary route is blocked. Again out-of-band routing might be necessary.

Requirement 5 implies partitioning of the network in security domains. Partitioning can be realized with or without the use of security systems. The partitioning of the network can be effected according to geographical, functional or organizational considerations. Here administration and other overheads must also be taken into account. An example is shown in Figure 5-16.

The figure shows all separating network devices in green. In principle, each separating device can be anything from an information diode or a simple filter in a router up to an advanced firewall or guard.

In a mission, accessibility between A and B might be more important than traffic from C or from the remaining network. This will be effected using suitable filters between A and B and between B and C.

In the figure, the combined blue network might be a network servicing an authority desiring the ability to protect parts of the net from outside traffic. Also shown is a limited amount of redundant routing in case of disaster.

5.5.2 Cryptographic methods

The purpose of the architectural view for cryptography is to support the use of methods for cryptography in order to insure the confidentiality, integrity under transmission, authenticity and non-repudiation of the information.

Safe distribution and revocation of certificates and keys require an architectural view for Public Key Infrastructure (PKI). The following components are required in the target architecture:

- Applications for PKI
- Network protocols for PKI
- Access to Certificate Authority (CA)

Presumably a solution based on COTS will be sufficient, but to allow for cooperation with coalition partners, the possibility of cross-domain certificates must be considered.

5.5.3 Confidentiality

The purpose of the architectural view for confidentiality is to ensure the confidentiality of the information. This can be obtained by logical or physical separation.

Logical separation is obtained by encryption, which may take place at all three layers of the DEFComm reference model:

- E2E encryption at the application layer - eg secure voice systems.
- E2E encryption at the convergence layer - eg by using IPSec.
- Encryption at the convergence layer to transportation between networks - eg by use of dedicated IP-crypto devices, or using IPSec.
- Link-encryption at the transmission layer - eg NATO approved encryption

All three encryption options are shown in figure 5-15. Please note that all options are shown, but they can be used independently of each other.

Physical separation can be used at the transmission layer of the DEFCOMM reference model. The media or network must be without risk for eavesdropping attacks, ie not available for unauthorized personnel

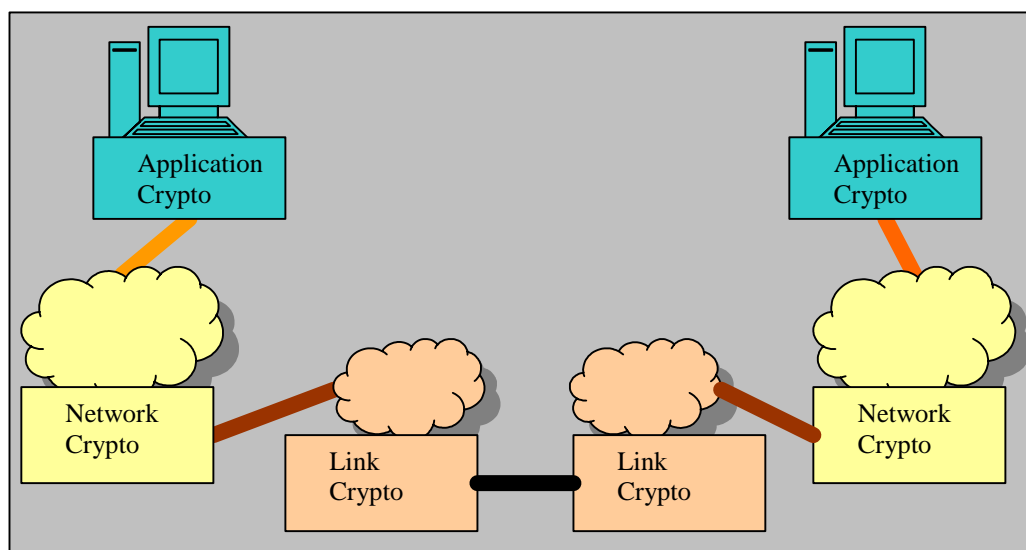


Figure 5-16: Examples of the positioning of crypto devices

The confidentiality architectural view considers the possibility of flexible partitioning of the infrastructure into red and black networks. The black network only carries black traffic, which may be either unclassified information or encrypted classified information. The red network may carry red traffic, which is unencrypted classified information. Thus the requirement that the core network must be black may be fulfilled. Approved crypto devices are required to secure separation and hence confidentiality. Regulations and available technology determine the details.

Compliance with military security regulations requires that the traditional separation of information into security domains and enclaves according to its classification must be respected in the target architecture for Danish Armed Forces communication. In principle, the partitioning can be the same as mentioned in the architectural view for availability. However, since the policies for information flow control may be different in the two situations, the partitioning may differ as well.

Current security regulations require physical or cryptographic separation of information according to national classification and corresponding classifications in NATO, the EU, etc. The classifications in question are:

- Highly classified networks for confidential and secret information
- Lower classified networks for restricted information
- Unclassified networks
- Public networks eg networks connected to the Internet

These networks can further be partitioned into:

- Internal networks, which according to function can be further divided into network for mission, education/training or welfare communication.
- External networks (from fully trusted to untrusted) including networks for communication with organizations outside the armed forces, eg local authorities or NGOs.

From a security point of view, a domain has no specific size. A domain may be anything from a single computer to a large network containing thousands of nodes. Even a network of networks can be configured as one single security domain or enclave.

The separation of domains and enclaves requires Boundary Control (BC) devices⁶, which include:

- Crypto devices including VPN-devices, where a transit network is used for communication between two other networks
- Information Exchange Gateways used for policy controlled communication between networks eg the use of firewalls, guards or other content based filters.

This should not prevent use of newer technologies becoming available, eg Content Based Information Security (CBIS).

5.5.4 Access control

The purpose of the architectural view for access control is to make sure that authorized users can get access to network resources while unauthorized users are denied access.

One requirement on this architectural view is that a single sign-on to a security domain will give access to all resources of this domain. Secure remote access to other security domains can be based on single sign-on if it is permitted by trust or by access policy. Access can be in the form of network access or user access.

Most elements for access control can be found at the service layer of the communication model. This includes:

- Applications or databases for registering users, rights, identification, authentication, etc.
- Verification of access on the basis of identity and policy. The policy may depend on the situation eg normal or mission.

Local and global aspects must be considered when the architectural view for access control is designed.

Access controls must include components at the convergence layer eg routers, management agents, etc.

The options for access control may change as newer technologies becomes available and dependable, eg the use of biometrics and smart cards.

5.5.5 Security aspects of NBO

Security is an important but often ignored precondition for NBO. The known security problems for platform-oriented operations will still exist for NBO, but priorities may change. For example NBO may tip the balance between availability and confidential-

⁶ Physical separation of the domains is obviously a much simpler possibility. However, physical separation is incompatible with the concept of NBO.

ity more in favour of availability. Also, NBO may call for larger networks than at present, and hence call for scalable solutions.

Security issues for NBO include (see [Ref 26]):

- Information Flow Control ie information control due to confidentiality or need-to-share concerns
- Problems concerning trust. Which users and which networks are to be trusted
- Dynamical changes caused by mobile or ad-hoc networking
- Scalable solutions for large and complex networks. It is essential that the solutions are scalable when many networks are to be connected
- QoS when using red/black partitioning, eg how can we ensure real time traffic, when information has to be encrypted?
- Availability including need to share versus confidentiality
- Authentication and non-repudiation in large dynamic networks

However, the whole concept of NBO is awaiting final development. One may safely assume that many more issues will emerge as the future brings newer developments of technology, principles and concepts for security. If priority of NBO increases, a new security architectural view based on NBO principles may be called for.

5.5.6 Concluding remarks on the security architectural view

The architectural view for security includes network partition into security domains and enclaves. Local availability and confidentiality are provided by security components inside the domains. Global availability is provided by redundant, robust and fail-tolerant systems and networks.

In order to provide confidentiality, integrity, authenticity and non-repudiation, PKI must be in place.

Administration and verification of access control must contain both local and global components.

The future development of NBO security architecture may impact the architectural view for security.

5.6 Network Management

The purpose of this section is to establish a Network Management (NM) architectural view. The architectural view will be based on key enabling technologies on network management. NM is a critical part whatever the nature of the network is, and NM is one of the essential building blocks of the target architecture. If all diverse networked infrastructures are not subject to the same (or even an improved) standard of management, existing networks will be unwilling to migrate and converge.

NM activity covers many areas of the network from straightforward monitoring of link status and controlling devices to traffic engineering built on statistics gathering and analysis, not only for future network planning, but also for other situations such as early detection of denial of service (DOS) attacks.

This elaboration of an NM architectural view is comprised of these parts:

- Brief outline of the NM concepts, its objectives, and the unique challenges future NM brings.
- Description of NM as a layered structure.
- Examination of key enabling technologies for network management.
- Transition towards the use of SOA for NM applications. This includes the aggregation of key enabling technologies in terms of distributed intelligence.

NM applications reside on the application layer of the DEFCOMM reference model, - however, the NM functions themselves cover all layers of the DEFCOMM reference model in an integrated way, - see details in the subsections below.

5.6.1 Network management concepts and objectives

With the increasing size and complexity of future networks, old-fashioned network management methods are no longer adequate and should be replaced with distributed management paradigms. By examining state-of-the-art enabling technologies, this section highlights some benefits, drawbacks, and postulates on a future network management architectural view. Despite NM diversity trends, NM is pushing towards distributed intelligence. NM agents are no longer treated as “dumb terminals”, but as sophisticated computing devices.

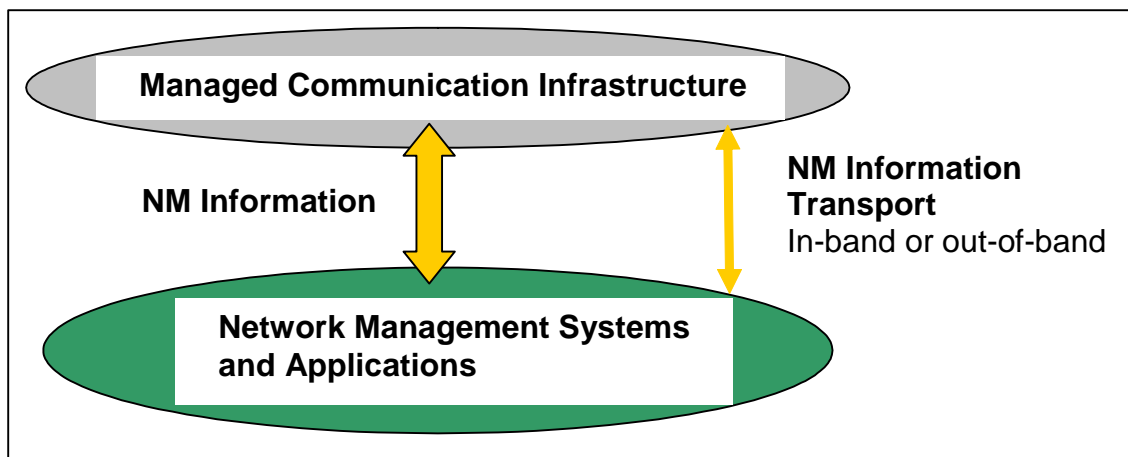


Figure 5-17: NM basic Architecture

The fundamental NM model consists of three basic components:

- The NM functions themselves, i.e. those functions which being used for managing of the communication infrastructure.
- Transport of Network Management information, either through the managed network or any parallel network.
- The NM systems and applications used for monitoring and controlling.

These three components are shown in Figure 5-17.

Transport of NM information is accomplished by NM protocols like SNMP, CMIT and CMOT that represent mechanisms which collect, change and transport NM information to and from destinations

5.6.2 Network Management reference model as a layered structure

As a general reference model for NM, the well-known Telecommunication Management Network (TMN) concept originally designed by ITU-T serves as the conceptual framework and terminology due to its more highly elaborated state than those of its roughly equivalent peers. In this section the TMN framework shall serve as the basis for referential integrity purposes only. This does not imply that TMN will be the basis for NM!

The model is often sketched as a layered structure with the most abstract components located at the top (operative management) and the more specialized physical devices (network elements) located at the bottom of the model. Every layer has its own functionality:

- **Operational management:** Relates to operational aspects such as mission planning and resource-allocation.
- **Service management:** Relates to user services including bandwidth management, storage and deployment of services.
- **Network management:** Technical management of all network devices including whole networks.

- **Network element management:** Relates to management of uniform network devices, ie groups of routers, bridges or gateways responsible for part of a network.
- **Network device management:** Relates to management of each network devices, ie routers, switches or hubs.

It is not possible to map directly between the layered TMN model and the DEFCOMM reference model. The NM functions works on all layers of the DEFCOMM reference model, and NM utilizes the transport services facilitated by the convergence layer and the transmission layer. In other words, NM is using facilities controlled by itself, - in principle this yields a recursive dependency, which should be minimized in order to avoid ambiguities. The relation between the functions of the TMN model and the DEFCOMM reference model is illustrated in Figure 5-18.

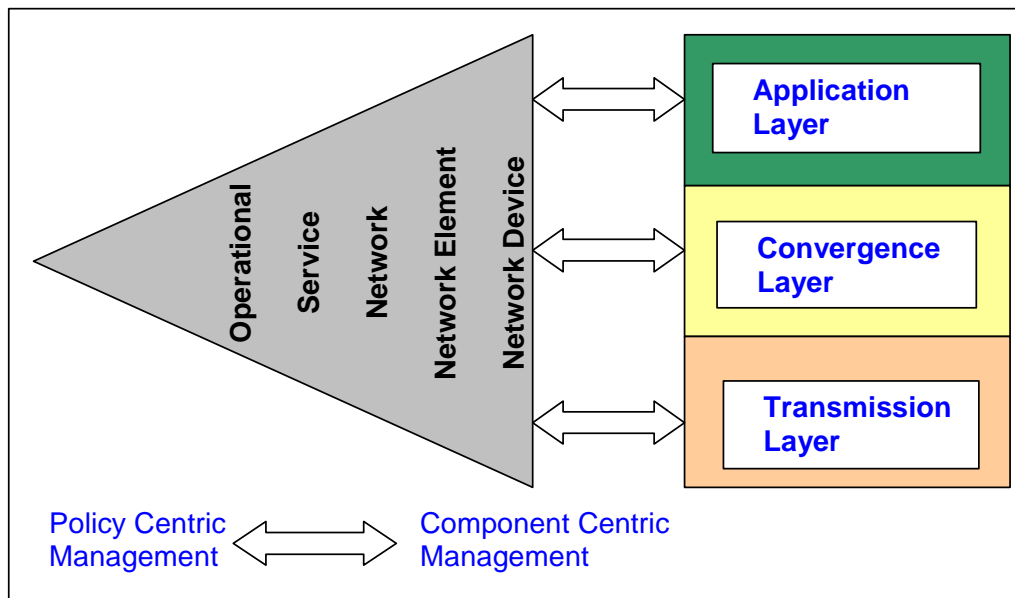


Figure 5-18: Layered NM functions related to DEFCOMM reference model.

5.6.3 Key Enabling technologies and protocols

It is a widely accepted fact that the evolution of NM functionality is towards distributed intelligence of management agents. A set of enabling technologies and protocols that are commonly recognized to be potential candidates for intelligent distributed network management will briefly be presented. The candidates are:

- Policy-based NM
- Distributed object computing
- Web-service based NM
- Code mobility for NM
- Intelligent (and mobile) agents
- Active Networks
- NM based on economic models

More details are in Appendix A: Enabling Technologies for Network Management.

5.6.4 Transition towards SOA

In general, networked infrastructure is moving from platform centric networks towards service-oriented approaches. Beside the NM objectives and OSI functional areas, NM has to fulfil additional management requirements, similar to today's military business service models, fast, deployable, mobility, service differentiation, service customizability, more features, and flexibility.

First of all, as the size of the networks is becoming larger, more and more network devices need to be managed efficiently, demanding better scalability on network management designs. As a result of such size increase, human directives can only be given at a very high level of abstraction and generalization in order to control the aggregated functionality and performance on each device. In other words, the underlying NM system must take care of the interpretation of these high-level directives to realizable network configurations.

This requires an abstraction level capable of monitoring the health (network health) of the whole network to a much higher degree than only details on each individual network device. Modern networks require an open management architecture with standard interfaces for information exchange between management systems and capable of managing large networks.

SOA has excellent properties for managing at a high level of abstraction as it is independent of the convergence and transportation layer in the DEFCOMM reference model and entirely lives a life of its own within the Information System Layer. SOA is in general assumed a better adaptation for NBO and thus this architectural view

Secondly, as networked infrastructures converge, heterogeneous network technologies must co-exist and cooperate. NM systems must provide such seamless integration via common service interfaces, and hide underlying technological heterogeneities from network users/administrators.

The transition towards SOA will be transition from network centric functions residing on the transmission and convergence layer towards high level abstraction NM-functions placed at the service layer of the DEFCOMM reference model. The NM is then turned over to be more user-centric in contrast to modern practice where NM-functions traditionally are residing at the three lower layer of the TMN model, i.e. network management layer, network element management layer and element management layer. These three layers are fundamentally component centric, aimed for monitoring, controlling and reporting on component basis.

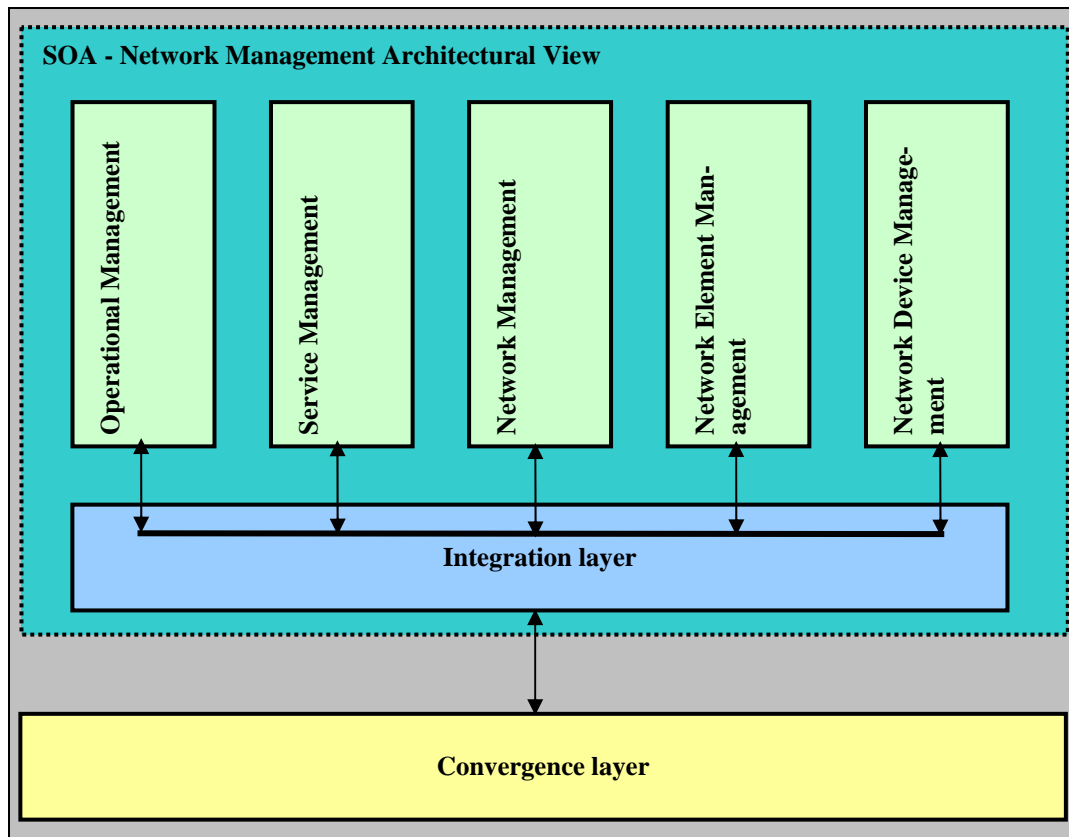


Figure 5-19: Network management referenced to SOA view

5.6.5 Concluding remarks

In this section, NM target architecture has been described. The NM architecture has been described in terms of a service oriented architectural view which facilitates NM functionality on high level of abstraction, independent from lower layer network devices. This facilitates NM on dynamic large networks in an efficient manner.

5.7 Addressing and routing

The objective of this section is to identify the architectural view of addressing and routing that supports NBO in a converged network. The need for a consistent and global addressing schema has arisen in order to ensure interoperability and reduce the requirement for system reconfiguration in the field. In addition to interoperability between forces, the Joint and Combined nature of recent and projected military operations in the future requires that any addressing standard includes Army, Air Force, Navy and other governmental organizations. Peacekeeping and other humanitarian assistance operations also require interoperability between military, governmental and non-governmental organizations. This section sets forth addressing target architecture (schema) that meets this requirement for military, governmental and non-governmental users.

5.7.1 Addressing and routing in the DEFCOMM Reference Model

As illustrated in Figure 5-20 the addressing is found both for communication and for information systems:

- Communication addressing takes place at the convergence and transmission layers of the DEFFCOMM reference model. The unified network addressing takes place at the convergence layer, - as an example the IP-addresses can be used as a unique global network addresses. The communication addressing is described in section 5.7.2
- Information systems addressing takes place in the service layer and integration layer of the DEFFCOMM reference model. The information system addressing is described in section 6.5.1.

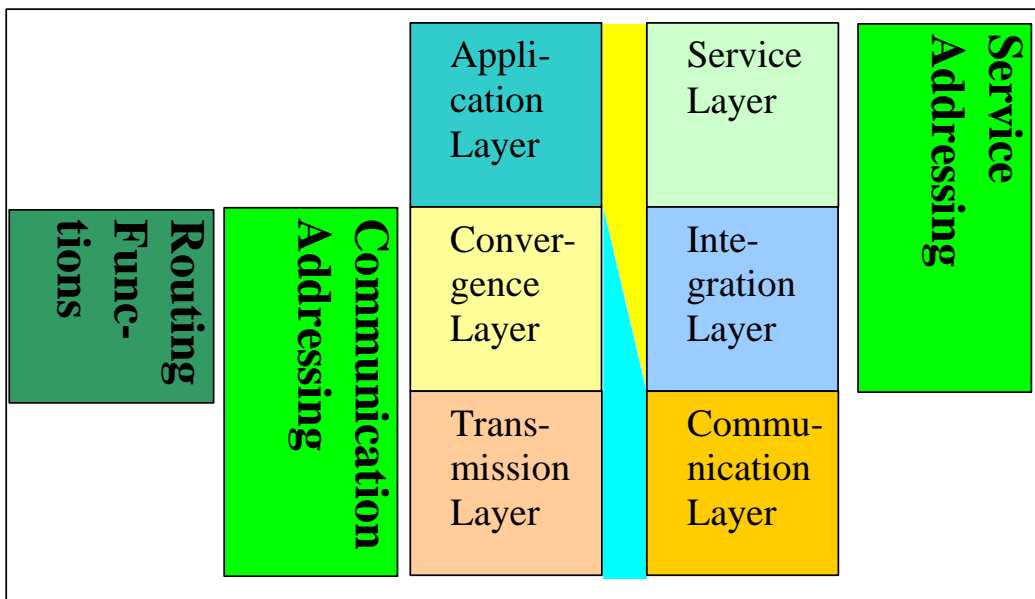


Figure 5-20: Addressing and routing within DEFCOMM reference model

There will be some overlap of addressing functions between the integration and convergence layers, - as an example we have mapping of hostnames into IP-addresses.

Closely related to addressing is routing which ensures the connectivity in a network. Routing is used to find the path through the network, and forward the information from source to destination. Network routing resides at the convergence layer only and is described in section 5.7.3.

5.7.2 Addressing mechanisms and functions

Addressing at the convergence layer means assigning local or global, private or public, temporary or persistent identifiers to network devices.

In this architectural view focus is set on some of the most popular network addressing mechanisms and functions, i.e.:

- Classful addressing means hierarchical addressing. Addressing without this mechanism does not scale well.
- Supernetting, also known as Classless Interdomain Routing (CIDR).
- Subnetting, i.e. use network device addresses as network addresses.
- Variable-length subnetting.
- Private addressing with network address translation (NAT). The private addresses are not available outside the local network.
- Dynamic addressing, i.e. network devices have an address assigned when the address is needed.

As an example this is well-known from IP-addressing, but the mechanisms and functions apply to other kinds of network addressing as well - such as telephony.

Although these mechanisms and functions all basically share the same theme (manipulating address space), they are different and should be used appropriately. When applying some of the listed addressing mechanisms, two things have to be emphasized:

- Network addresses and masks must scale to the sizes of the areas to which they will be assigned.
- Establishment of some degree of hierarchy in the network.

In order to scale the network addressing, a number of different network address domains should be considered, including:

- Functional areas (FAs) within the network.
- Workgroups (WGs) within each FA.
- Subnets within each WG.
- All the subnets (current and future) in the organization.
- All the devices/hosts (current and future) within each subnet.

By establishing the scaling and hierarchies for the communication infrastructure, we are applying addressing, not only system-wide but also across FAs, WGs, and subnets. The intent here is to look at addressing from many perspectives so that we do not lose the detail of any particular area and do not fail to see the overall addressing picture. While each of the addressing strategies could be applied to any area of the network, there are areas where each strategy is more appropriate. Figure 5-21 shows where each strategy may be applied.

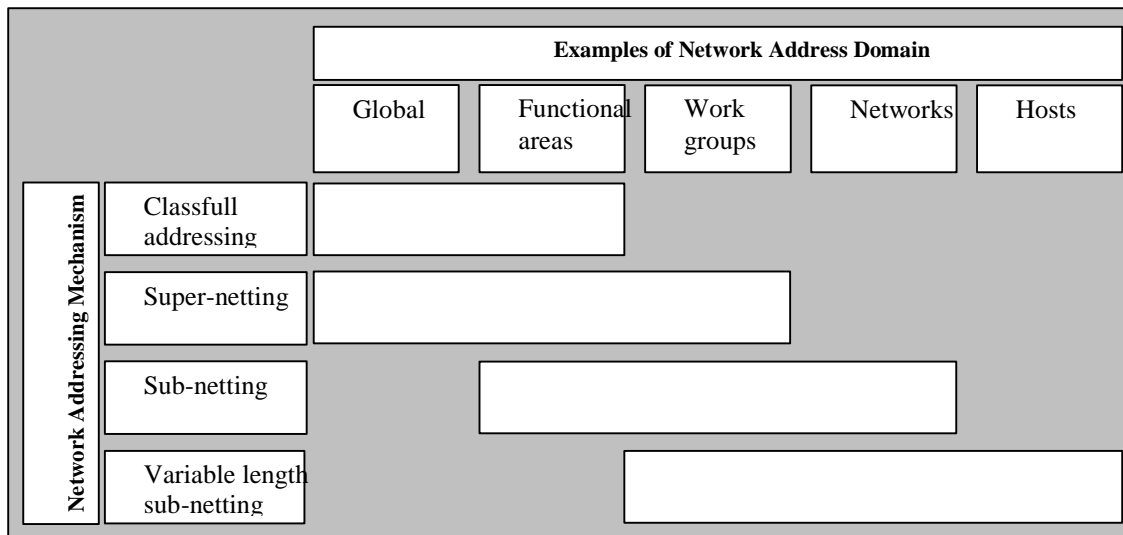


Figure 5-21: Applying various addressing strategies

There is an increasing trend toward mobile networking, so a static addressing model is inappropriate, and some means of dynamic configuration is required.

On larger networks and inter-networks it is also likely that a naming service will be offered to provide a form of yellow pages directory service. In fact, with the scaling up of networks and the emergence of tools such as firewalls and dynamic dial-up VPNs, there is a need to configure and manage policies for features such as authentication, QoS, configuration data, and bandwidth. Huge amounts of data are being centralized and coordinated via directory services and protocols such as the Lightweight Directory Access Protocol (LDAP). The functions mentioned in this paragraph all resides on the application layer, but mapping to addressing functions at the convergence layer is needed.

Specific addressing at the transmission layer is not part of the target architecture, but address mapping from convergence layer is needed, in particular with networks of networks, such as transmission networks and VPNs.

5.7.3 Routing Mechanisms and Functions

Routing architecture shall provide the functionality for finding the path through the network and for forwarding the information from source to destination. The information to be routed is both user data and management information, including the routing information needed to discover the path through the dynamic network.

Thus routing consists of learning about the connectivity within and between networks and applying this information to forward data toward its destination(s). Routing in combination with the addressing element of the architecture provides a complete picture of network connectivity.

Typically routing protocols are considered somewhat apart from what is normally considered as network performance metrics, such as routing convergence times; their protocol overheads, in terms of capacity (bandwidth), CPU utilization, memory utilization; and stability. Although these are important characteristics to consider, it is

often difficult to relate them directly to the network architecture or design. Routing protocols are, however, indirectly related to the architecture through two characteristics, namely hierarchy and interconnectivity.

To fulfil the principal objective of the DEFCOMM target architecture, the routing-architecture must take into account how current and future systems will be connected using a variety of local, metropolitan, and wide area networking technologies; the topology of interconnection will change as systems and the links between them are added and deleted (including MANET); the networks will cross every conceivable national and international boundary; and the systems and networks will be administered by different organizations, both public and private, each of which may impose rules (policies) governing (and safeguarding) their use. Thus the target architecture for routing should:

- Scale well for network of networks, thus supporting NBO.
- Support many different network types and multiple Qualities of Service.
- Adapt to topology changes quickly and efficiently, ie with minimum overhead and complexity.
- Provide controls that facilitate the secure connection of multiple organizations.

A routing scheme for a large-scale open systems network must be dynamic, adaptive, and decentralized; be capable of supporting multiple paths offering different types of service; and provide the means to establish trust, firewalls and security across multiple administrations and domains.

5.7.3.1 OSI Routing Architecture

The following discussion of routing in the target architecture is based the OSI routing framework [Ref. 27] due to its connection-oriented behaviour as is for the TCP protocol. By doing this, the conceptual framework and terminology of OSI forms the consistent basis for a deeper understanding of the subject.

Like all routing schemes, the OSI routing scheme consists of:

- A set of routing protocols that allow end systems and intermediate systems to collect and distribute the information necessary to determine routes
- A routing information base containing this information, from which routes between end systems can be computed. Like a directory information base, the routing information base is an abstraction; it doesn't exist as a single entity. The routing information base can be thought of as the collective (distributed) knowledge of an entire subsystem concerning the routing-relevant connectivity among the components of that subsystem.
- A set of routing algorithms that use the information contained in the routing information base to derive routes between end systems

End systems (ESs) and intermediate systems (ISs) use routing protocols to distribute ("advertise") some or all of the information stored in their locally maintained routing information bases. ESs and ISs send and receive these routing updates, and use the information that they contain (and information that may be available from the local environment, such as information entered manually by an operator) to modify their routing information base.

The OSI routing architecture is hierarchical, and is divided into three functional tiers:

- End-system to intermediate-system routing (host-to-router), in which the principal routing functions are discovery and redirection.

- Intradomain intermediate-system to intermediate-system routing (router-to-router), in which "best" routes between ESs within a single administrative domain are computed. A single routing algorithm is used by all ISs within a domain.
- Interdomain intermediate-system to intermediate-system routing (router-to-router), in which routes are computed between administrative domains.

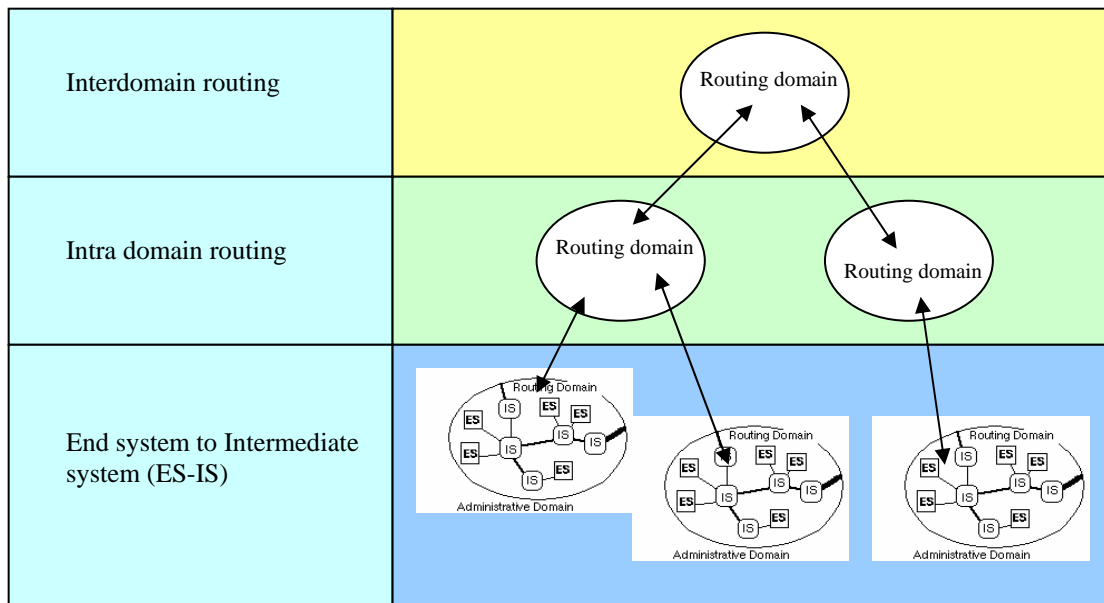


Figure 5-22: Hierarchical relationship of the OSI Routing Architecture

In Figure 5.22, end systems discover and communicate with the intermediate systems to which they are directly connected (by dedicated or dial-up point-to-point links or by multiaccess local or metropolitan area networks) in the outermost level of the hierarchy; intermediate systems communicate with other intermediate systems within a single routing domain in the levels of the hierarchy next closest to the centre; and in the centre, intermediate systems communicate with other intermediate systems across routing domain boundaries. In the OSI routing architecture, end systems are not involved in the distribution of routing information and the computation of routes as is for eg the Internet.

It should be emphasized that analysis leading to one conclusion in the intradomain context not necessarily hold when transplanted to the interdomain context and vice versa.

Within the OSI routing framework, it is possible for different routing domains within a single administrative domain to run different intradomain routing protocols, and it is also possible to operate different ES-IS protocols within different areas of the same routing domain.

5.7.3.2 TCP/IP Routing Architecture

Through a process of evolution-in which some of the ideas that led to features of the OSI routing architecture originated with TCP/IP, developed into OSI standards, and returned to be adopted by the TCP/IP community-the TCP/IP routing architecture today is almost identical to the OSI architecture. Hosts use a discovery protocol to obtain the identification of gateways and other hosts attached to the same network (subnetwork). Gateways within autonomous systems (routing domains) operate via an interior gateway protocol (intradomain routing protocol), and between autonomous systems, they operate via exterior or border gateway protocols (interdomain routing protocols). The details are different but the principles are the same as for the OSI routing architecture.

5.7.3.3 Routing in MANET

Mobile Ad-hoc networking (MANET) enables ad-hoc temporary wireless networks composed of mobile nodes. Routes are set up and maintained by a routing protocol. MANET routing protocol design is a complex issue considering the possibly rapidly changing topology of such networks. For route maintenance traditional protocols used in hardwired networks cannot directly be used in the sense that no single protocol can fit all the different scenarios and traffic patterns of MANET applications. It is very likely in future MANET applications that it will be possible to combine one or more competitive schemas to fulfil application needs. In MANETS the hosts participate in the routing. Routing in MANET is still a fruitful area for research.

5.7.4 Concluding Remarks on Addressing and Routing

Addressing and routing provide the basic functionality for forwarding user, and network management traffic through the network. In developing the addressing/routing architecture, the addressing and routing must reflect the hierarchy and interconnectivity of the network which is very important for the operational functionality of the overall performance of the network. Routing domains may be controlled by different administration policies where issues of security (including control over the extent to which information about the topology of one domain is propagated to other domains) can be in contradiction. When selecting an intradomain routing protocol, concealing or withholding information, is often as important as distributing it, in order not to infer misleading information on the network health.

5.8 Network Based Operations (NBO)

The purpose of this section is to set forth an architecture that addresses NBO, potentially enabled by operational architectures that closely integrate the capabilities of sensors, command and control, and effectors. Consequently the NBO architecture can be drawn by examining operational architectures that effectively link sensors, command and control, and effectors in order to increase joint and combined combat power.

In principle the NBO related functions reside on the application layer of the DEF-COMM reference model; - however, the NBO functions need support by the communication infrastructure. The information, sensor, and engagement networks of NBO may be supported by virtual networks (or grids) facilities at the convergence layer. These grids may be logical or physical networks.

5.8.1 Information Network

The information network (or information grid) provides the infrastructure for network based processing and communications. This infrastructure provides the means to receive, process, transport, store, and protect information for the joint force. The information network, shown in Figure 5-23, is a network of networks consisting of communications paths ("links" and "pipes"), computational nodes, operating systems, and information management applications that enables network-centric processing and communications across the joint battle space. The information network provides a multi service architecture.

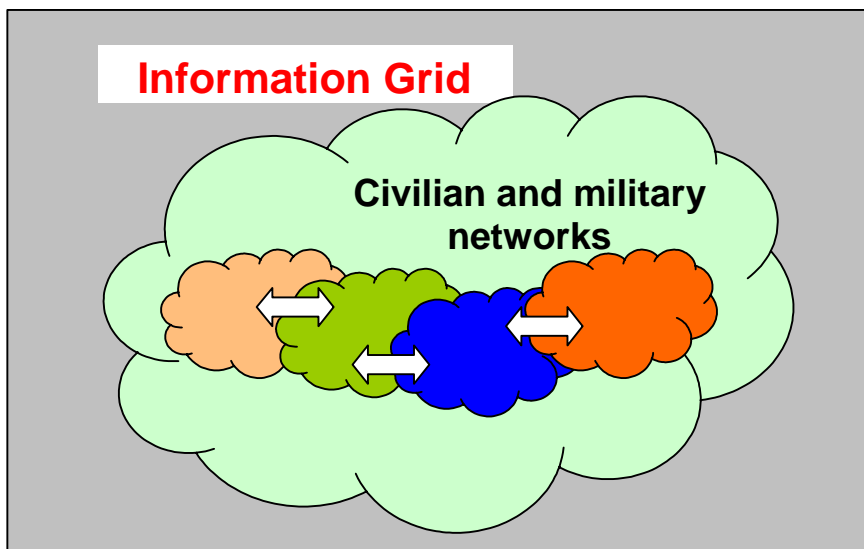


Figure 5-23: The Information Network Architecture

The information network consists of both military and commercial communication capabilities and transmits multiple information types in multiple modes at multiple data rates. Voice, data, and video can be transmitted via point-to-point or direct broadcast in wired and/or wireless mode.

Another key capability of the information network is information protection which enables the information network to provide assured access to information across all levels of conflict by preventing intrusive attack and assure commanders that their information will be valid.

5.8.2 Sensor Network

Sensor networks (or sensor grids) are composed of air, sea, ground, space, and cyberspace based sensors. Elements of sensor networks include dedicated sensors, sensors based on weapon platforms, sensors employed by individual soldiers, as well as embedded logistics sensors. Sensor networks provide the joint force with a high degree of awareness of friendly forces, enemy forces, and the environment across the joint battlespace.

Sensor networks provide the joint force with the operational capabilities necessary for achieving awareness across the joint battlespace. Abstractly, sensor networks can be viewed as sets of *sensor peripherals* and *sensor applications* that are "installed" on the information network. The sensor "peripherals" consist of space, air, ground, sea, and cyberspace based sensors. These sensors can be based on dedicated sensor platforms, weapons platforms, or deployed by individual soldiers. The sensor peripherals also include embedded sensors that track levels of consumables (ie, fuel, munitions). The sensor network applications consist of the software applications associated with specific sensor peripherals, as well as the software applications that enable multi-mode sensor tasking and data fusion. The operational performance is achieved through a combination of dynamic sensor tasking, data fusion, and effective distribution of information over the information network in real or near real time. The sensor network is depicted in Figure 5-24.

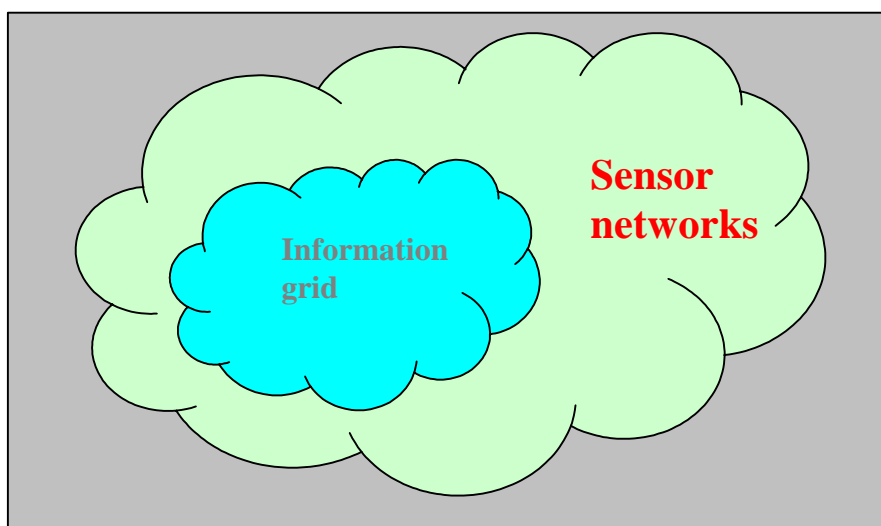


Figure 5-24: Sensor Network architecture

5.8.3 Engagement Network (effector network)

Engagement Networks - the operational architecture of engagement networks enables the joint forces to employ speed of command effects at precise places and time.

The operational architecture of engagement networks, depicted in Figure 5-25, effectively exploits battlespace awareness to enable new operational capabilities for force employment. These new operational capabilities for force employment enable the emerging operational concepts of precision engagement, dominant manoeuvre, and full-dimensional protection.

These new operational capabilities include:

- Predictive Planning and Pre-emption. - The ability to be proactive in the planning process to avoid direct confrontation (by employing alternative means), to be prepared to react and exploit opportunities when direct confrontation must occur, and to shape expected actions to stay inside an enemy's decision cycle and keep him outside of ours.
- Integrated Force Management - The ability to achieve dynamic synchronization of missions and resources from components and coalitions.
- Execution of Time-Critical Missions - The ability to enable rapid target search and acquisition.

As with sensor networks, the engagement networks can be envisioned as a set of *shooter peripherals* and *shooter applications* that operate on the information network. The engagement network peripherals consist of effectors based in air, land, sea, and cyberspace. The shooter network applications consist of the software for command and control and weapon employment.

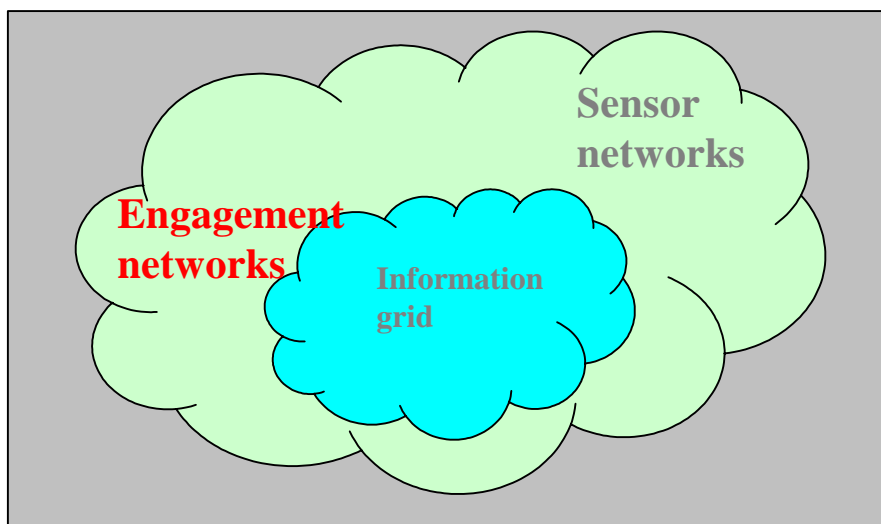


Figure 5-25: Engagement Network architecture

5.8.4 Concluding remarks on NBO

In conclusion, we can see that the emerging concept of Network-Centric Warfare provides an organizing principle in terms of the emerging operational architectures of the information network, the sensor network, and the engagement network as described above. This description provides a point of departure for exploring how the individual components of our existing and emerging forces can be integrated to enable the network-centric operational concepts.

5.9 End-to-end Communication

The aim of this section is to introduce a generic *end-to-end* (E2E) architectural view. This view is of relevance to communication scenarios where separate units of the Danish Armed Forces are connected to disjoint networks and have to communicate with each other through one or several transit networks.

The characteristics of transit networks may differ widely, which to some extent may influence the transparency of the communication service. Tactical or strategic regards may call for specific levels of Quality-of-Service (QoS) or security. When requirements for QoS or security have to be met, every net in the communication chain must be able to support the demands in question. When the specific transit networks are not known beforehand, progressive Service Level Agreements (SLAs) must be used to find a route that can guarantee the desired levels of QoS and security.

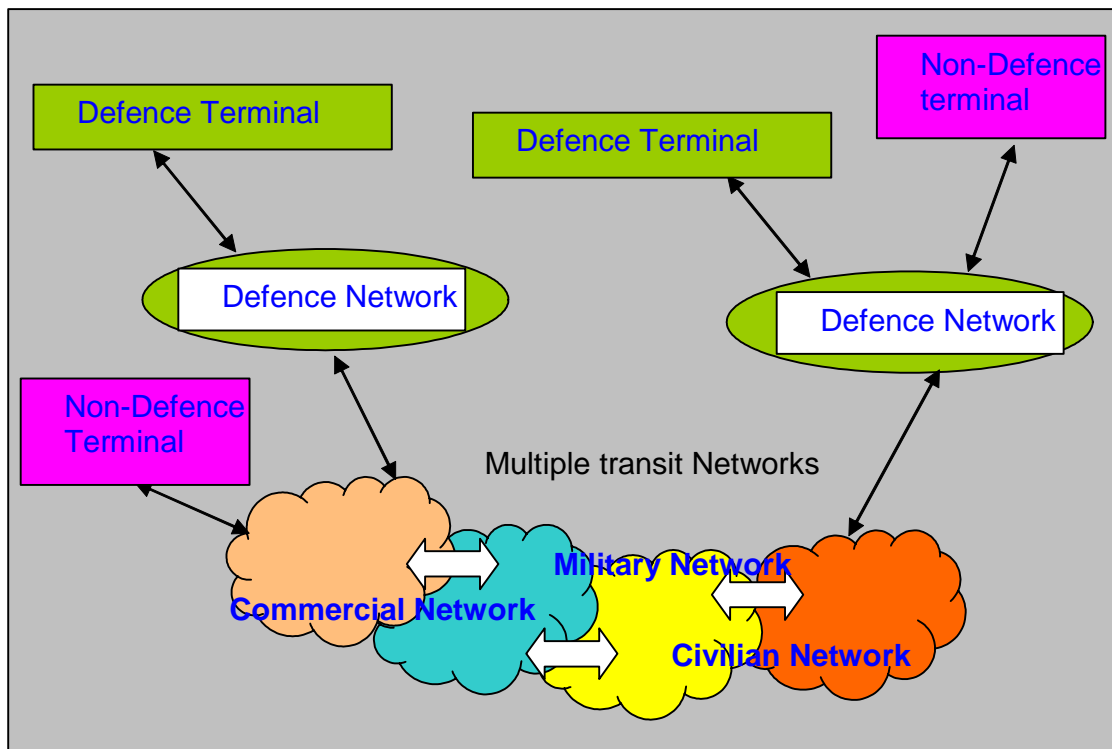


Figure 5-26: End-to-end communication between defence and non-defence enterprises

In E2E communication part of the communication chain may be controlled by entities outside Danish Armed Forces, eg by coalition partners, public or private authorities. We may wish to consider the following cases of E2E communication:

- Both communication ends inside the Danish Armed Forces
- Sender inside the Danish Armed Forces, Receiver outside
- Sender outside the Danish Armed Forces, Receiver inside
- Both communication ends outside the Danish Armed Forces (relevant when Danish Defence provides communication support to foreign entities, whether civil or military. May occur in case of a regional conflict or natural disaster)

Also the transit networks may be outside Danish Armed Forces control. Here we must consider separately if

- Network is owned and operated by a foreign entity.
- Network is owned by the Danish Armed Forces, but is run by a foreign entity.

The target architecture must allow one or more of its elements, whether communication sender, receiver or network to be outside the control of the Danish Armed Forces. These aspects have profound implications not only upon E2E communication accessibility, security, and QoS, but also upon the actual running of the communication networks.

Figure 5-26 illustrates an architectural view of various possible E2E communications.

5.9.1 Concluding remarks on the E2E architectural view

The E2E architectural view is of relevance for homeland defence as well as for Danish Armed Forces operations far from the homeland. The Danish Armed Forces may here need to use much diversified communication channels, such as local communication systems, rented circuits, satellite connections, etc. In addition, the upcoming concept of NBO may call for an extensive ability to use various combinations of any networks at hand for transit. It is important to find a communication solution that will allow especially transit networks to be controlled and operated by units outside the Danish Armed Forces.

5.10 Communications Evolution

The purpose of the communication evolution architectural view is to show how it is possible to evolve from current military communication systems (mid 2005) to the target architecture based on all-IP communication, eg the evolution architectural view is a road map over time for transition to the target architecture.

The view is shown as four snapshots starting with the current situation and ending up with the target architecture which represents the long-term aiming point for military communication. However, it must be emphasized that the transition is a continuous process; - the four snapshots are only used to indicate a possible road.

The snapshots are shown without absolute time, because the transition time towards the target architecture depends on the technological development⁷. It is estimated that within 10-15 years it is possible to reach the target architecture from a technical point of view - or at least come close.

It is assumed that the evolution ends up with a converged network based on the IP-suite; however, the IP-suite is still being developed and therefore the IP-suite could very well differ from what is known today. The IP-suite development is mainly expected in the civilian world, including known problems regarding QoS, Security, and management. This development should of course be taken into account in the evolution architectural view.

5.10.1 Snapshot 1, Initial architecture (today)

The initial architecture shows the current situation for military communication systems, - yet with a degree of generalization. The networks used are heterogeneous where each network has associated application services and transmission mechanisms. Exchange of information between the dedicated application services has to be done manually or by use of dedicated gateways.

Related to the DEFCOMM reference model the initial architecture with the current situation is illustrated in Figure 5-27.

Architecture	Communication architecture description (exclusive tactical links)	Tactical links
DEFCOMM Reference Model		
3 – Application Layer	Application specific services including gateways	Native TDL services
2 – Convergence Layer	Dedicated networks	
1 – Transmission Layer	Dedicated transmission mechanisms	

Figure 5-27: Initial Architecture (snapshot 1)

⁷ Other issues may apply as well, eg economy.

5.10.2 Snapshot 2, Pre-NBO architecture (mid-way 1)

The pre-NBO architecture shows the situation where communication can be seen from an IP point of view, ie a core-IP network is available as basis for building static and dynamic infrastructures to fulfil requirements of current military operations and tasks.

All networks are heterogeneous and they have their own associated application services and transmission mechanisms which still are usable for the original operational purpose. The networks can exchange information by use of gateways as there will still be a need for exchange of information between dedicated application services.

An exception from the IP point of view is tactical data links (eg LINK 16) or other systems which can not easily be integrated into the IP-suite. Also dedicated facilities not yet supported by the IP-suite (eg QoS) must be supported outside the IP-suite.

Related to the DEFCOMM reference model the pre-NBO architecture (the mid-way 1 situation) is illustrated in Figure 5-28. All networks are heterogeneous and have their own associated application services and transmission mechanisms.

Architecture	Communication architecture description (exclusive tactical links)	Tactical links
DEFCOMM Reference Model		
3 – Application Layer	Application specific services including gateways	Native TDL services
2 – Convergence Layer	Core-IP network Dedicated networks	
1 – Transmission Layer	Dedicated transmission mechanisms (+ IP transmission mechanisms)	

Figure 5-28: Pre-NBO Architecture (Snapshot 2)

5.10.3 Snapshot 3, NBO prepared architecture (mid-way 2)

The NBO prepared architecture shows the situation where communication takes place with one of these methods:

- An IP converged network, and other networks can be used as a transmission mechanism.
- Network-gateways make it possible to exchange information between networks where IP is used as the network protocol, and other networks. This makes it unnecessary to exchange information directly between the dedicated application services by using dedicated gateways.

All networks are heterogeneous with their own application services and transmission mechanisms.

The tactical data links may be integrated as well, but the future use of these must be clarified and the needed gateways developed. The alternative is still to regard them as autonomous networks; yet, use of tactical data links as transmission mechanism for IP-traffic should be possible.

Related to the DEFCOMM reference model the NBO prepared architecture (the mid-way 2 situation) is illustrated in Figure 5-29. All networks are heterogeneous and may have their own associated application services and transmission mechanisms; however, they can all be used as transmission mechanisms for the IP-infrastructure.

Architecture DEFCOMM Reference Model	Communication architecture description (exclusive tactical links)	Tactical links
3 – Application Layer	Application specific services (including NBO support)	Native TDL services
2 – Convergence Layer	IP converged network (+ Dedicated networks including gateways)	
1 – Transmission Layer	IP transmission mechanisms (+ Dedicated transmission mechanisms)	

Figure 5-29: NBO prepared Architecture (Snapshot 3)

5.10.4 Snapshot 4, NBO supported architecture (target)

The NBO supported architecture shows the situation where all communication takes place in an all-IP converged network. Other networks are only used as a transmission mechanism or they must be equipped with network-gateways for working together with IP-networks. In principle all networks can still be heterogeneous and each of them can have their own associated application services and transmission mechanisms; however, all information exchanges must take place through gateways. Exchange of information between dedicated application services through dedicated gateways should not be necessary- and hence no longer supported.

The tactical data links are integrated parts of the network; however, the target architecture includes the possibility of having gateways (between tactical data link systems and IP-systems) with full functionality. Also, the tactical data links may still be used as transmission mechanisms for IP-networks.

Related to the DEFCOMM reference model the NBO supported architecture (the target architecture situation) is illustrated in Figure 5-30. All networks are heterogeneous and may have their own associated application services; however, all services must comply with the all-IP network.

Architecture DEFCOMM Reference Model	Communication architecture description
3 – Application Layer	Full NBO support + Application specific services (incl. TDL)
2 – Convergence Layer	All-IP
1 – Transmission Layer	IP transmission mechanisms

Figure 5-30: NBO supported architecture (Snapshot 4)

5.10.5 Concluding remarks on evolution

The evolution architectural work shows a possible road from current communication architectures towards the target architecture. It is important to notice that the evolution should be a continuous process over the whole period. In the near future, the current and new systems must co-exist, - yet they are used as dedicated systems. The change of paradigm occurs when the systems can be viewed as an IP-converged network, thus the communication is part of the NBO concept.

5.11 Mobility

The purpose of this section is to look into the mobility perspective of the target architecture in the form of a mobility architectural view. The mobility architectural view shall mainly consider the user requirements for mobility. The characteristics of mobility are divided into two separate aspects:

- Degree of mobility for terminals
- Degree of mobility for whole networked infrastructures

The architectural view shall facilitate mobility in the operational mode ie operational on the move as well as timely discrete mobility carried out via physical mobile platforms. Additional mobility requirements in terms of Ad-hoc networking shall be supported.

The mobility architectural view assumes that optimal network and E2E connectivity exist at any time. Mobility can be divided into the following mobility types:

- Mobility of individual terminals. This means transparent communication between terminals and/or users.
- Mobility of Networks. This means movement of whole networks by means of edge-devices belonging to another network of networks while maintaining total transparency.
- Mobility of applications (logical mobility). This means absolute availability of applications all over the entire network.

Regarding the DEFComm reference model mobility is accomplished at the convergence layer and includes mobility for heterogeneous transport networks. Due to support of mobility at the convergence layer mobility support at the application layer is automatically supported. Additional mobility may be performed E2E at the application layer however this is outside the scope of WP3, as is the use of mobile code.

At the transmission layer, mobility functionality depends entirely upon individual transport mechanisms ie wireless technology supporting roaming facilities. This kind of mobility is proprietary for each manufacturer and is transparent from the convergence layer point of view. In case of mobility requirements from operational users, mobile mechanisms at the transmission layer must be available.

Mobility can be classified according to different criteria.

- Geographical coverage: ie local, regional or global mobility of terminals and networks. Micro mobility typically includes local and to some extent regional communication. Macro mobility supports global coverage. Micromobility can be exemplified by Mobile Ad-hoc NETworking (MANET) and Macromobility by Mobile IP (MIP).
- Functional coverage: ie defined role models based on services. This logical mobility requires characteristics of both terminals and networks to support different roles and require specific functions at the convergence layer.

This is shown in Figure 5-31. The geographical movements are shown with block-arrows, and the functional mobility is shown by colour codes. The networked infrastructure shown includes convergence layer with matching transmission facilities.

A networked infrastructure supporting mobility must have several functionalities of which the most important ones are:

- Mobility functions at the convergence layer by means of addressing (naming and network addresses, geographic location, etc.), re-routing, management, roaming between different transmissions facilities, setup and configuration for mobility, continuous sessions, etc. This could be constituted by an intelligent mobile agent.
- Mobility at the transmission layer by means of wireless mechanisms supplemented by necessary roaming possibilities such as GSM, LAN, Bluetooth, Wi-Fi, WiMax, and Zig-Bee (sensor network).

A critical aspect of the mobility architecture is the requirement for dynamic scaling due to the tremendous amount of terminals that is expected to be supported by the mobile infrastructure.

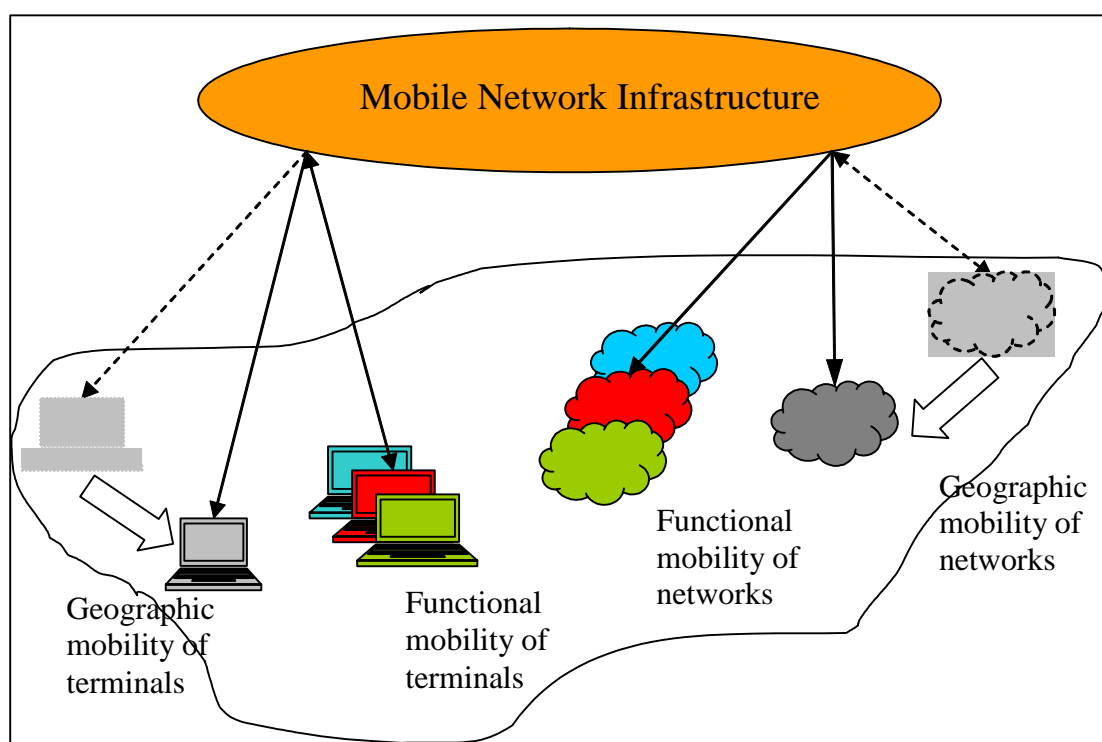


Figure 5-31: Mobility supporting architecture

5.11.1 Concluding remarks on mobility

An infrastructure supporting mobility should offer the same services as fixed networks although there may in a foreseeable future still be limitations due to characteristics of some mobile transport mechanisms eg bit-rate limitations. This implies that certain mobile services will be constrained with regard to some QoS requirements. In NBO, the mobility requirement is a prerequisite which also impacts the DEFCOMM target architecture.

5.12 Other Communication Architectural Views

This section will summarily mention a few other architectural views which may have a role to play in the final communication *systems architecture*, even if these views don't have much influence at the current stage of planning.

VoIP – Voice is an important part of any military communication, and VoIP will be a decisive factor in any IP-based target architecture. We may here distinguish between VoIP and IP-telephony, of which only the latter will require the use of normal telephone facilities, such as telephone calls, exchanges, trunk lines, etc. Assuming sensible choices are made regarding telephone facilities, and assuming satisfactory levels of QoS can be obtained, both VoIP and IP-telephony may be of interest to Danish military communications.

MPLS backbone – MPLS (or its more recent relative: GMPLS) may be an integral part of the convergence process towards an all-IP network, in which case MPLS routers (switches) must be deployed in a suitable structure.

Campus Communication – This view describes communication in camp, eg for Danish military units that are deployed abroad. These units will need communication internally as well as externally, with headquarters in Denmark, with allied forces nearby, with local military and non-military authorities, as well as welfare communications with family at home. All these forms of communications are included in other architectural views, such as

- 5.1 Local, Regional and Global communications
- 5.3 A global information network
- 5.5 Security⁸
- 5.9 End-to End Communication

DEMARS Communication – DEMARS may very well make its own specific demands on the communication system architecture. This has not been analyzed in depth. Our assumption is, that all DEMARS communications demands are met by the proposed target architecture. Sufficient accessibility to the central databases of DEMARS will in all likelihood be assured by the proposed global information network. A closer analysis regarding local or regional use of DEMARS may be warranted to ensure existence of proper transmission capacities.

Tactical Data Links - The important concept of Tactical Data Links (TDL) is only peripherally discussed in this report. Only those aspects of TDLs that are relevant to the individual architectural views described are considered. The reader is referred to other reports for more details regarding TDLs, also in connection with NBO.⁹

⁸ Here especially the separation of military and non-military communication is important

⁹ Ref 23 (in Danish) "Link 16 I Forsvaret, FOFT LINK 16 Studie" may serve as a starting point for more detailed information on Link 16 as well as TDLs in general.

6 Application Architectural Views

In this chapter a number of different architectural views assessed to have significant impact on the target architecture for the military application and information systems are described. In general the level of details is somewhat limited compared to the communication architectural views. This is mainly because of the broader scope of the target architecture for applications due to the lack of precise requirements gained from WP2.

The sequence in the description does not necessarily imply priorities. Furthermore, each architectural view (subchapter) can be read independently of one another. This implies to some extent overlap between the descriptions of each individual architectural view. However, this structure makes it is easier to relate system architectures to the target architectural views.

For each architectural view the following items are described:

- The specific purpose of this part of the architecture.
- The scope and environment, including the relation to the DEFComm reference model.
- The requirements to be fulfilled by the view itself

Most of the architectural views are analysed with regard to their properties, advantages- and disadvantages. The expected technological evolution and its impact in the timeframe of this study are included as well.

The information Systems Reference model in Figure 3-3 describes three layers, which from top to bottom are called service-, Integration- and communication layer. The lower layer will primarily be provided by an IP-based network. The two upper layers will be based on a service oriented architecture, which will enable a loose coupling of services. The use of service oriented architecture will be an important facilitator when realizing Network Based Operations. In the following sections, we will describe the service oriented architecture concept and part of the web service technology. The latter is currently the preferred technology used to implement service oriented architectures.

6.1 Service Oriented Architecture (SOA)

In this section the aspects of SOA as a part of the target architecture are discussed. First the SOA concept is introduced, then how SOA can be implemented in existing military applications. Finally there is a subsection introducing the web service technology, which is currently the preferred technology used to implement SOA.

6.1.1 SOA Introduction

Service Oriented Architecture (SOA) is a set of architectural design principles, which governs the design of loosely coupled software systems. The main components of service oriented architecture are loosely coupled autonomous services, which are solely defined by and accessed through their interfaces. An autonomous service is a software component that implements a business process, and in this sense it is dif-

ferent from traditional objects and components. Since the service is only defined by the interface, a service consumer does not need to know the inner workings of the service, and a service can therefore be both platform and implementation language agnostic. Service oriented architecture is different from application architecture, since the former is more focused towards a specific set of customers and a specific situation, where the SOA is more generic and in this role favours reuse by different communities of interest. Service oriented architecture is therefore not a replacement of other architectures, but is an architecture which only deals with all the aspects of the service level of an architecture. A major goal of service oriented architecture is to align IT capabilities with business processes and not the other way around, which often has been the case in the past. The enterprise view of an SOA describes only the standards based interfaces of the underlying system and is a higher level of abstraction which focuses on the implementation of business processes [Ref. 25].

In service oriented architecture a service is made available by a *service producer* and the service is used by a *service consumer*. The only interaction between the producer and the consumer is done via the *service contract* as illustrated in Figure 6-1, and the consumer will therefore be able to use the service, without any knowledge of the implementation of the particular service. These SOA components resides on layer A (the service layer) of the DEFCOMM reference model.

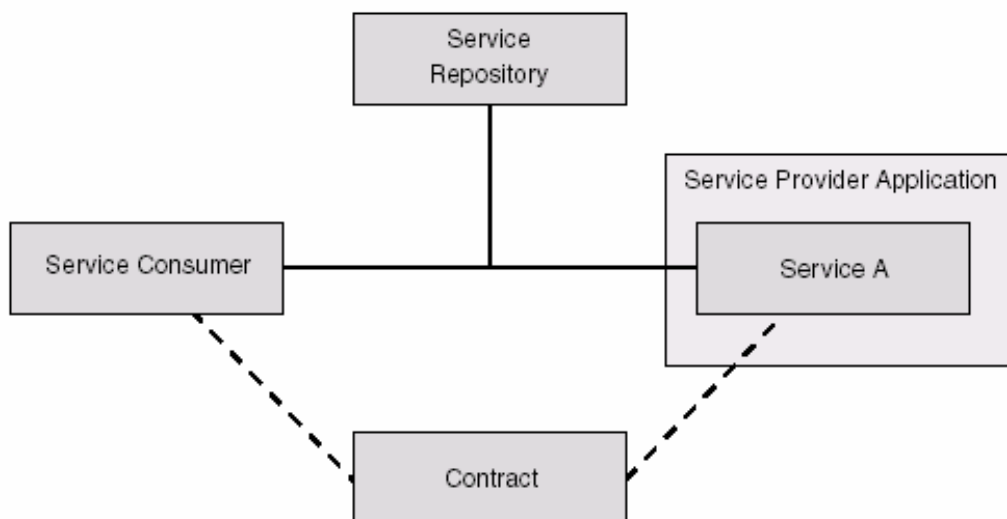


Figure 6-1: The three types of components in an SOA [3] and the contract

NATO and DoD have traditionally described an architecture using operational-, system- and technical views to illustrate the different aspects of an architecture. In today's platform oriented architecture, there will be a tight coupling between operations and systems, and for that reason there will often be a direct mapping between operational requirements described in the operational view and the functional components described in the system view. In a service oriented architecture, the introduction of an enterprise service view will separate the operational view from the system view. In service oriented architectures, the operations will drive the services and the services will drive the system, and will therefore effectively decouple the operational view from the system view.

The main principles, which govern the design of service oriented architectures, are:

- **All business processes are modelled as services** - The central concept of service oriented architecture is the service. Services implement domain-

specific business processes and are designed for reuse by other applications in same domain. When defining a service, it is important simultaneously to define the scope of the service, so that reuse can take place outside the scope of the current application.

- ***A service is solely defined by its interface*** - A service is only defined by and accessed through a well defined interface, which is defined in a vendor and platform independent way. Separating the interface from the implementation of the service, enables consumers to use a service on a different platform, created in a different language, and even more important, enables the consumer to utilize a service, without having any previous knowledge of the inner workings of the service.
- ***Services are autonomous*** - Being autonomous means that the service is self-contained, has its own performance criteria etc. A service should also be meaningful to the consumer, when certain business functionalities are implemented. The service should be implemented in such a way, that the service can easily be substituted by a similar implementation, without affecting any service consumers. In general, the service should provide the necessary interface to provide reuse and loose coupling.
- ***Services should be loosely coupled*** – A loosely coupled service enables a complete separation between the service consumer and provider. Loose coupling enables cleaner separation of the user interface from the underlying technology used to implement a service, and allows the consumer to compose a system using multiple heterogeneous services.

6.1.2 Service Implementation

Services may be implemented as a pure SOA service, but as SOA is gradually implemented, a large number of services will be wrapped legacy components. Besides being a producer, a service may also act as a consumer of other services. It will be up to the producer of services which services should be published, and which service should be internal to a specific domain.

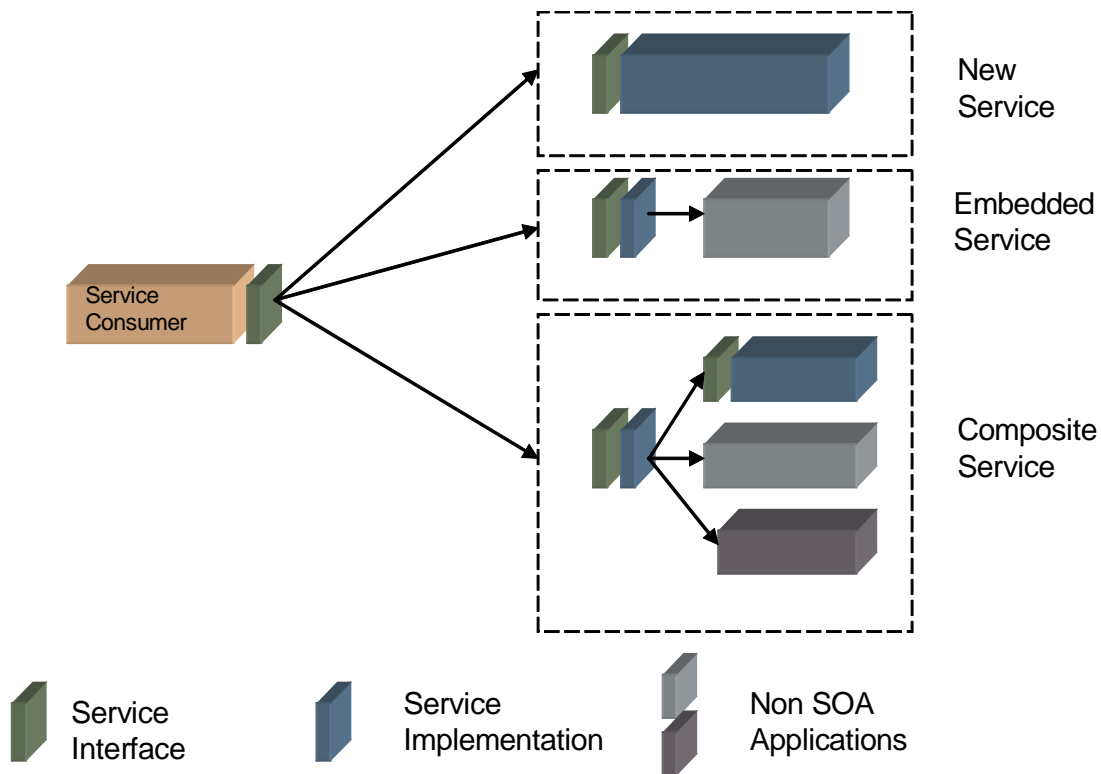


Figure 6-2: Service composition and orchestration (adapted from [Ref. 3])

Figure 6-2 illustrates the three main kinds of service implementations, namely a new service, a legacy application that is wrapped, ie given a service interface, and a combined service consisting of legacy and new service components [Ref. 3].

Future application development will to a large degree be done by composing services in a plug-and-play fashion, using concepts like orchestration and composition, which are defined below:

- **Orchestration** – is the composition of multiple services in order to create a business process reusing existing services. The resulting service can therefore be regarded as a simple process, which in it self can be considered as a service.
- **Choreography** – deals with collaboration between multiple services, which is part of a larger business process. Choreography therefore deals with the exchange of messages between multiple parties in a peer-to-peer fashion.

These functionalities must be available at layer A (the service layer) of the DEF-COMM reference model.

6.1.2.1 Web-Services as enabling technology for SOA

Since the service oriented architecture is only an abstract description of the underlying business processes, it is necessary to select a platform on which the services can be implemented. The platform of choice for now is the Web Service platform. The term platform is a bit misleading, since the web service platform is actually a collection of standards, APIs and specifications, which implement a common infrastructure

that service producers and consumers can rely on. Being standard based also frees the implementation of vendor lock in, and enables interoperability across both platform- and organization boundaries. Although web services are currently the default platform used to implement service oriented architecture, it is important to realize that using web service will not automatically enforce the service oriented architecture- the architecture needs to adhere to the basic SOA design principles.

The basic web service platform consists of the following standards, which implements a number of technologies for message transport, service description and service discovery:

- **XML** - XML is the format of choice, when defining the data that will be exchanged between the consumer and producer of an application. XML enables the consumer and producer to exchange information in a vendor neutral way.
- **SOAP** – SOAP is an asynchronous message protocol, which can be used to send messages between a service consumer and a service provider. SOAP is transport protocol agnostic, meaning that it may use several transport protocols such as HTTP, SMTP, FTP, etc. SOAP is extensible so that external standards can be utilized in SOAP.
- **WSDL** – The service level contract describes the interface of the service. The interface must be the only access point for a service and can be defined using the Web Service Description Language (WSDL). It is not mandatory to describe the interface using WSDL, but in order to promote reuse; a description of the interface is required. Otherwise, the service will not be discoverable.
- **UDDI** – To be discoverable, a service needs to be registered in a service repository, The Universal Description, Discovery and Integration (UDDI) specification is a way to register and discover web services. UDDI has not been widely adopted and is currently not recommended.

These technologies reside on the layer B (integration layer) of the DEFCOMM reference model.

6.1.2.2 Additional Web service functionality

The Information System Reference model illustrated in, Fig. 3.3 defined a number of additional functions required, when implementing a SOA. Among these are:

- Web service process, incl. flow languages and tools for choreography and orchestration
- Service implementation frameworks
- Service description languages
- Server communication standards

A number of the information service functions are relevant across both the service and integration layers. These are:

- **Service Registry**: The service registry allows service providers to register service and service consumers to discover services. A service registry is essential for the use of SOA. Typically WSDL is used to describe the service and a UDDI registry is often mentioned as a potential candidate for an SOA

registry: however, the standard is still considered immature and might be replaced in the future.

- **Transaction:** When orchestrating a number of services, transaction becomes very important. A transaction mechanism ensures that a system is kept in a consistent state, and provides recovery facilities if necessary.
- **Service (including Information) Management:** Management of services will be just as important as management of the underlying communication infrastructure. A number of management proposals currently exist.

Web service security is becoming increasingly important. However the web-services security landscape is still immature, although significant progress has been made in recent years.

6.1.2.3 Web services in perspective

The advantages and disadvantages of SOA in the form of web services are exposed in [Ref. 13], where the following points are discussed:

- Vendors, ie what is the supply situation for the technology
- Cost, ie what is the cost by purchase and wide spread use of the technology?
- Openness, ie are there implementations based on open, non proprietary standards?
- Maturity, ie at which development stage is the technology?
- Evolution potential, i.e. does the technology seem to be promising in the sense that it may be an important vehicle for NBO in Denmark?

The reader is referred to Appendix B for a more detailed walk-through.

6.2 Applications Evolution

This section contains a road map for the transition of the applications to the target architecture. The evolution must be seen in conjunction with the evolution of the communications, because the applications and their integration will be heavily dependent on the availability of communication services. However, as the communication is dealt with elsewhere (section 5.10), it is throughout this section assumed that the communication infrastructure is in place.

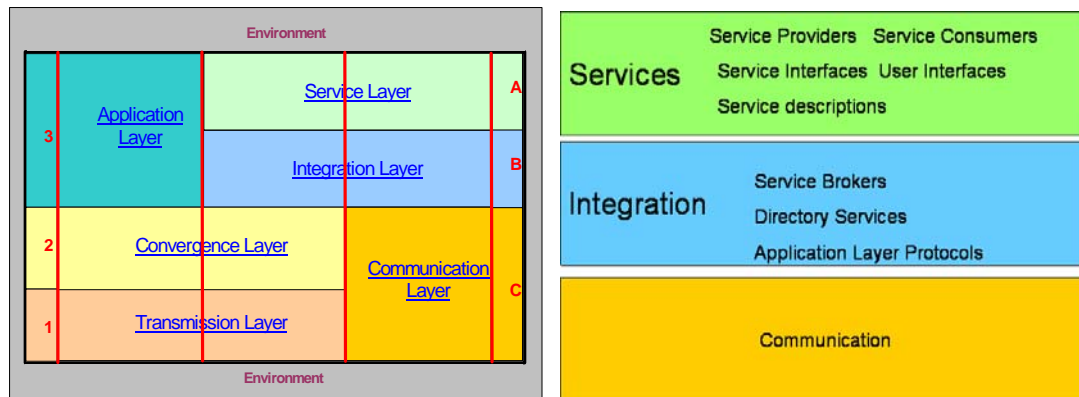


Figure 6-3: Information System part of the DEFCOMM reference model in more detail.

The information systems target architecture is in principle an all Service Oriented Architecture. This means that all applications and data that are to be shared are published as services and accessed through their defined and described interfaces. The interfaces are coarsely grained, so that a service is a meaningful and independent part of a business process. It must, however, be emphasised that there will be many applications that are not service oriented, simply because their functionality will be of no use or interest to remote entities. Trivial examples are office applications like Word and Excel, less obvious examples are dedicated applications like calculations of fire solutions, process controlling SW, and services from basic software like the operating systems of the computers. As for now, the service oriented architectures cannot fulfil real time requirements. Real time systems may be exempt from being implemented in SOAs because of that.

The development towards the target architecture may be divided into three stages, approximately covering 5 years each.

At the first stage, covering the period from now (2005) until the year 2010, the development will be characterised by the following items:

- Standards for service descriptions and service brokers must be selected.
- Methods for acquisition, development, and managing services must be developed.
- All new applications with functionality or data that are to be distributed will have as an option to be service oriented at the end of the period. The possibility of service orientation will be a requirement on all new ICT acquisitions, and there must be a waiver if they can not be implemented in an SOA. They will have the option to be implemented as web services.
- A few old applications should be wrapped so that they can meaningfully be shared as web services. Candidates are parts of the CCIS of the three ser-

VICES and parts of DEMARS. These applications may serve as demonstrators, and thus pave the way for further successes.

- The rules and principles for the military SOA are established. Applications that follow these rules are *net worthy*. The rules must be in accordance with the rules of anticipated coalition partners.

At the next stage, the period 2010-2015, the feasibility and added value of SOA have been demonstrated. This stage is therefore characterised by:

- All new applications with functionality or data that are to be distributed will be service oriented, in the sense that they follow the rules that allow them to be part of the military SOA. The possibility of service orientation will be a requirement on all new ITC acquisitions except for the dedicated or real time systems, and there must be a waiver if they cannot be implemented in a SOA. *Web Services* is the most likely platform.
- Old systems will be wrapped in the sense that they will be given interfaces that allow them to be part of the military SOA.

The final stage, reached approximately in 2020 presupposes a further technological development that allows more systems, including real time systems, to be implemented in service oriented architecture. At this stage security problems, management of these systems of systems and human computer interaction problems have hopefully been solved. This means that almost all shareable resources are accessed as services. It is not obvious that web services will be the preferred vehicle at this stage!

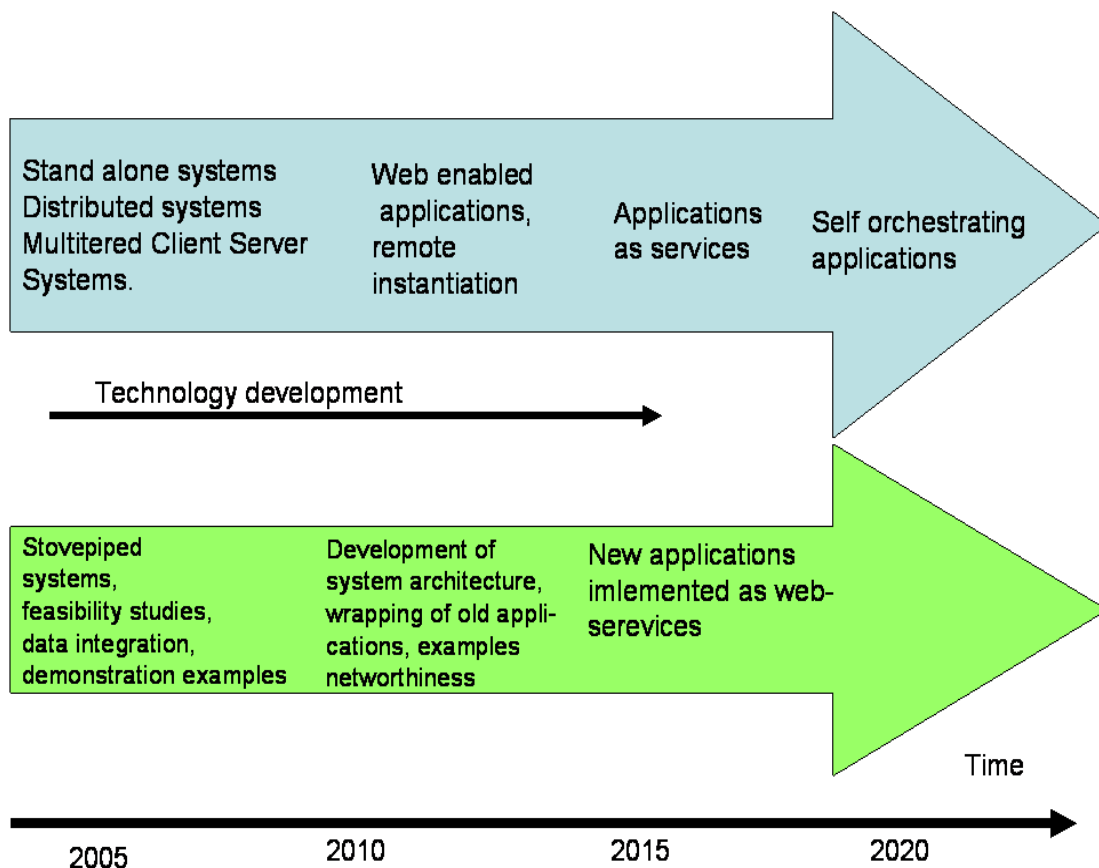


Figure 6-4: Technology development and roadmap

Figure 6-4 shows the expected development of the technology for making distributed systems compared to the stages outlined above.

Security properties become particularly important. The commercially available mechanisms for authentication and authorisation in Web Services are developing fast, but they are still not considered sufficiently reliable for military use. New ideas such as Content Based Information Security (CBIS) are promising, but not really mature yet.

6.3 Services and applications in NBO

The purpose of this section is to set forth an architecture that addresses NBO potentially enabled by operational architectures that closely couple the capabilities of sensors, command and control, and shooters. Consequently NBO architecture for applications can be drawn by examining operational architectures that effectively link sensors, command and control, and shooters in order to increase joint combat power.

Network based operations advocates a Service Oriented approach for information distribution and management and rejects doctrines that dictates some predefined strict flow of information exchange as in traditional military hierarchies. Instead, services and application related to NBO resides on the service and integration layer of the DEFCOMM reference model. However, NBO services and functions need support from the lower communication layer in terms of logical and physical communication paths. The SOA approach to NBO is sketched in Figure 6-5.

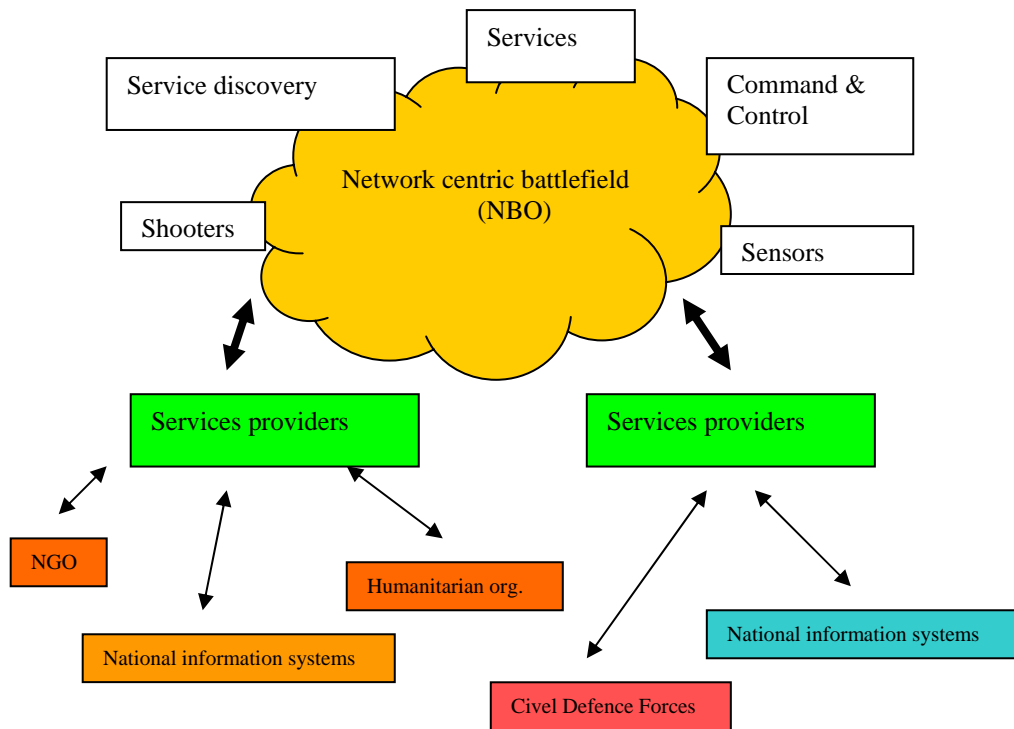


Figure 6-5 The SOA approach to NBO

6.4 Information Management

One important aspect of NBO is the sharing of information. SOA exposes information to users (consumers) through the service interfaces. This means that information management is performed at the service level, and thus not important for the target architecture. However, in the more detailed system architecture information management is a key issue.

6.5 Naming services

The purpose of this section is to describe a naming and addressing structure in a service oriented environments. This naming service is established on the service and integration layer in the DOFCOM reference model.

6.5.1 Addressing in a Service Oriented Architecture environment

Addressing in SOA is closely related to discovering and providing services. Addressing is therefore a two step process, where step one is locating a service repository, and step two is requesting and obtaining the service. In both steps an addressing scheme is a necessity.

One of the major principles of SOA is the service registry. A service registry enables registration of services and enables services to be discovered. The service registry must contain information of all available services, how to address them and a description on how services are utilized. SOA will provide seamless and transparent access to services. However, the concrete technology used to implement SOA, will define how services are located and addressed and might very well be implemented differently on various platforms.

In many present scenarios, however, messages are targeted directly to a service, and the addressing information in the message simply using an URL. However messages shall not necessary be limited to specific addresses.

In obtaining the above addressing concept the addressing mechanism within the Service Layer in the DEFCOMM reference model must provide a transport-neutral service addressing mechanism. This Service Layer addressing mechanisms enables services and applications to support message transmission through networks that include processing nodes such as endpoint managers, firewalls, and gateways in a transport-neutral manner e.g. decouples address information from any specific transport model.

Controlling the addressing schema combined with a transport-neutral encoding of the message source and destination enables SOA enabled Service messages to be sent across a range of transport networks, through intermediaries, and it enables both asynchronous and extended duration communication patterns as well as real time communication.

Addressing mechanisms in a SOA environment also enables a sender to indicate where a response should go in a transport-independent manner. The response to a message may not necessarily go to the sender. In HTTP for example, without any SOA like addressing it is impossible to specify that the response should be sent elsewhere.

Addressing mechanisms for SOA implementations provides a general mechanism to associate incoming or outgoing messages with specific tasks. The mechanism that the service uses is transparent to those using the service through an endpoint reference. Examples of basic addressing mechanisms in the Service Layer are Directory Services and Domain name services.

6.6 Application Security

An architecture based on SOA principles must also include a security component, which will deal with security at the service level. The service component should therefore not replicate security mechanisms, which exists at the integration or communication layer of the reference model.

Among other things the SOA security component should:

- Manage security policies associated with a service
- Handle identity management
- Establish authentication mechanism for access to services
- Enable trust relationships between services
- Signing of messages

The functionality mentioned above covers among others, the security concepts of confidentiality, integrity and non-repudiation. A SOA security component must also support availability by providing functionality similar to what is described in the communication part of the target architecture (see section 5.5). In the availability can be ensured by the following requirements.

- Robust service implementation, and potentially a redundant service infrastructure
- Reliable messaging between services
- Management agents able to monitor and control the services. N.B. Only internal services can be controlled in this way. External services must be secured by other means and eventually have fallback mechanisms.

The service level security component would need to be integrated with security components located at other levels of the reference model, such as PKI, directory services, etc.

6.7 Some Other Application views

User friendliness and human computer interaction (*HCI*) in general are essential for the application layer. The usability issues are far more complex than just “Using the browser and WWW techniques” seems to indicate. This view comprises issues from design of screens and forms, ease of learning, to use to multimode interfaces.

Scalability is also a must at the application level. Scalability has at least two dimensions, one is the number of users, the other is the geographic reach. A number of the usual commercial solutions may have scalability problems.

Applications may usually be classified (grouped) according to their weight on *functions and algorithms*, on *information*, and on *timeliness*. The first group is well represented by scientific computing, where relatively few data are used in complex calculations. One proposed solution to this is grid computing, which seems to converge to SOA. The second group is represented by large administrative systems, where enormous amount of data is used as input to simple calculations, and where the data load in the output stream also may be high. The third category consists mainly of systems with hard or soft real-time requirements. The SOA approach may not be well suited to this category, because of the loose coupling and hence little control flow between service consumer and service provider.

7 Synthesis- Bringing It All Together

The previous chapters have discussed a number of architectural views. The set of views form the building blocks of the target architecture. In this chapter, we deal with the concatenation of the views and the problems associated with the dependencies between the views. The views themselves comprise several sub views in their own rights. This is eg the case for the Local/Regional/Global view, the IP-convergence, the security view, and the NBO view. We do not in this chapter go through all the views, but consider only the ones deemed to be the most important with regard to the proposed target architecture.

7.1 *IP contra non-IP and other forms of dependence*

The communications target architecture is based on a transition towards an all-IP network, but many views are independent of the IP-suite. It is therefore of interest to identify which components are dependent on the IP, and which are not. The independent components can be exchanged without modifying the convergence protocol.

It is obvious that the IP-convergence is dependent on IP, but the network addressing, the address structure and most of the routing share this dependence. The evolution toward an all-IP network and the involved architectural views are also dependent on IP. Most of the other views are not dependent on IP.

An important example is the application architecture, which will converge via an SOA. The basic SOA principle is not dependent on the network protocol. However concrete implementations such as Web Services rely on the IP-suite. In an SOA, the security properties become particularly important. The commercially available mechanisms for authentication and authorisation in Web Services are developing fast, but they are still not considered sufficiently reliable for military use. New ideas such as Content Based Information Security (CBIS) are promising, but not really mature yet.

The QoS view is one example of problems that may be introduced by the IP. The present versions of IP are connection less (best effort) protocols, which means that they in principle are non-deterministic. It is therefore in principle impossible to guarantee a certain level of service, eg real time performance, in a communication based on IP.

Also the security, specifically the availability properties, will be hard to guarantee. It should be noted that the commercially available IP-encryption methods are not accredited to be used for military data classified above restricted today. A development in this respect is expected along the lines of the US work on High-Assurance-IP-Encryption (HAIPES), where military applications are foreseen. Public key encryption is already in commercial use for transmission of certificates etc., and will be important for large parts of the administrative systems. A similar public-key-infrastructure is being developed in NATO and will eventually also be implemented in the military infrastructure.

8 General Aspects of the Architecture of Defence ICT systems

In this chapter the target architecture and its advantages, disadvantages and limitations are discussed.

8.1 *IP as protocol for Communication Convergence*

It is without doubt that the convergence architecture is to be based on the IP-suite and IP-compliant software and hardware. The reason for this is the dominant position on the commercial market that this protocol has and the availability of COTS based on it. In the military market the IP-suite is gaining interest eg as the protocol for Global Information Grid (GIG) and the one advocated for in the NATO NEC Feasibility Study [Ref.4].

One of the IP-protocol advantages is that it can be used on many types of transmission channels eg Ethernet, WAN, ATM, SATCOM, UHF etc.

Other advantages of the IP-technology include the non-functional properties:

- Many suppliers
- Many types of products
- Low cost
- Fast development cycle
- Closely connected to market requirements
- Widely implemented, huge technology base
- Many interfaces to the IP from other protocols in existence

It has to be noted that the IP-technology for the moment is not able to fulfil all the requirements for the military network. The target architecture incorporates for these reasons autonomous systems eg TDL and VHF/UHF radio in the IP-network. Use of gateways allows communication to be made between the IP-network and the autonomous system.

The current research and development of IP-technology is aimed at removing the current constraints in IPv4. We see in IPv6 that QoS facilities have been added and the address space has been extended.

8.2 *The use of other protocols than IP as protocols for convergence*

A number of other protocols or protocol schemes may support the IP convergence. These include:

- **ATM** which satisfies most QoS requirements by design. Even if the commercial penetration is limited ATM might function as the backbone of a high performance network. Tunneling of IP-traffic through ATM is a standard solution

- **SONET/SDH** (Synchronous Optical Networking/Synchronous Digital Hierarchy). Communication based on optical fibre typically used as convergence layer in the telesector for voice and IP-traffic.
- **MPLS**. Packets are encapsulated and transmitted through a tunnel which guarantees that the actual network route is known. In this way QoS and near real time can be obtained in an IP-network. MPLS does not scale well and cannot be recommended for the convergence network. MPLS development is taking place eg GMPLS.
- Other proprietary protocols might be used for dedicated purposes with connection to the IP-networks through available gateways. Other proprietary protocols might be used as a transmission layer for IP-traffic under the assumption that a tunnel solution exists. Due to their limited use, these protocols can not be recommended for the convergence network.

8.3 Gateways in general terms

In this report, the term *gateway* so far has been used without an explicit definition. The term generally means a hardware and software device for the conversion of information. In principle, the purpose is to convert information and maintain its properties eg richness and actuality etc. between two networks. In reality, the gateway functionality is limited to the least common denominator of the two networks. The actual limitations depend on the gateway implementation.

Since the use of gateways causes information and/or information properties loss, the use has to be as limited as possible. In the NBO context, it is important that the gateway solutions are scalable and that only one gateway type is used per application or system that cannot directly be connected to the network. Also, in an NBO context, it is important that the gateway functionality is automatic and not based on human intervention, eg converting telephone voice to UHF radio.

In the context of the IP-convergence architectural view, gateways are used to connect non-IP based networks to the IP-infrastructure. Such a gateway can be one-way or two-way and offer more or less functionality. In one end of the spectrum we see fully integrated two way gateways which are able to transparently enlist a device from a non-IP network as a complete and valid device on the IP-network and vice versa. End users from different networks will be able to communicate as if they were on the same network.

An example of a fully integrated two-way gateway is a VHF radio – IP gateway (see section 5.2.3). An end-user using a PC with a headset is able to communicate with another user on VHF radio. The communication is transparent to the users.

At the other end of the spectrum gateways with limited functionality exist. Typically the purpose is to make information from non-IP networks available on the IP-network. This can be done by connecting a device (eg a standard PC) on the IP-network to a native device on the non-IP network. The signals in question eg the situation picture are connected to the PC and through the use of standard software transmitted to the IP-network. In its simplest form such a gateway can be a PC with a webcam. The camera is aimed at the situation picture and voice is lead to the voice recording device on the PC. Picture and voice are presented on the IP-network using standard web technology.

In the context of TDL it is worth noticing that if full functionality is required, the gateway has to comply with the specifications such as IERs for the TDL. Configuration and upgrades have to be made to the gateway in the same manner as the native devices on the TDL and information has to be presented using standard technologies eg web, XML etc.

8.4 Target architecture compliance with communication requirements

The choice of target architecture is a result of the requirements stated in WP2 [Ref. 2]. Most of the architectural views are related to WP2 where requirements are described.

In WP2 requirements from generic tasks are converted to technological requirements in the form of local communication, communication between C2 systems, BLOS communication, naming and addressing, real time communication, visualizing and controlling communication, etc., and these requirements are reflected in the architectural views as described in chapter 5.

Requirements for tactical and strategic communication are directly reflected in the LRG architectural view, while the requirements of NBO communication are reflected in the universal and NBO architectural view.

The target architecture does not prevent the use of a network based function for time and position tracking. However, the system architecture has to specifically address the topic as well as the software defined radio and VoIP topics.

8.5 Concluding remarks on general aspects of the proposed architecture

The broad application and dominant position of the IP-suite on the market makes it the suite of choice for the convergence layer ie the layer with which other networks and TDL are to be connected. The problems of QoS which the IP-suite faces might be solved by the use of supplementary protocols. However hard real time requirements can only be satisfied in dedicated networks eg TDL. Gateways are the glue between IP-networks and non-IP networks and can have more or less functionality.

9 The Target Architecture (top-level)

In this chapter the **Target Architecture** (TA) for the Danish Armed Forces is drawn up from a top level point of view. The starting points of the TA are the technology projected on expected development, a networked infrastructure with the Internet Protocol (IP) as convergence protocol, the SOA of information systems (including applications), and integration of services with a loose coupling.

The convergence ensures a communication environment where multimedia, voice, video and data are integrated in a unified communication system with IP as the main network protocol, and thus yields the full benefit of the IP-suite. This means that network devices can interact directly with each other, - yet the actual interaction may be limited by security, capacity, and for other reasons. The network convergence in a distributed environment makes it possible to have local, regional and global communication between all systems and applications. Both information and services can reside on distributed servers and may be used by all users on the network. The military TA based on network convergence will fully support NBO with sensors, effectors and C2-systems. Furthermore, this TA is easier to design, deploy, support and maintain than a heterogeneous networked infrastructure.

Service integration ensures an information systems structure where the services have a well-defined interface to the integration functions. This means that the services can be domain-specific for the Armed Forces and still have a loose coupling with other services – enforced by the integration.

The prerequisites for the description of the TA are the architectural views described in chapters 5 and 6 together with the considerations in chapters 7 and 8. The TA top-level architectural views are drawn in these subsections:

- Section 9.1 with the integrated architecture of both applications and communication infrastructure.
- Section 9.2 with more details of the application architecture.
- Section 9.3 with more details of the communication infrastructure architecture.

All together, the TA shows that the information processing systems and applications can be distributed by seamless use of the communication and application infrastructure. The top-level view of the TA in this chapter is supported by more specific details in the architectural views described in chapters 5 and 6. System architecture for the Danish Armed Forces can be evolved from the target architecture by providing more details both on the top-level views and the specific architectural views.

9.1 Top-Level Target Architecture

This section describes the target architecture for DEFCOM at top-level. The **Top-Level Target Architecture** is the first step in a top-down approach to define the complete target architecture. The top-level architecture is described in two steps, - first as a general protocol independent architecture (section 9.1.1) and then integrated with the IP-suite as the chosen convergence protocol (section 9.1.2).

9.1.1 General Top-Level

This section describes the target architecture as a **General Top-Level** sub-architecture. The top-level architecture is the first step in a top-down approach to define the complete target architecture.

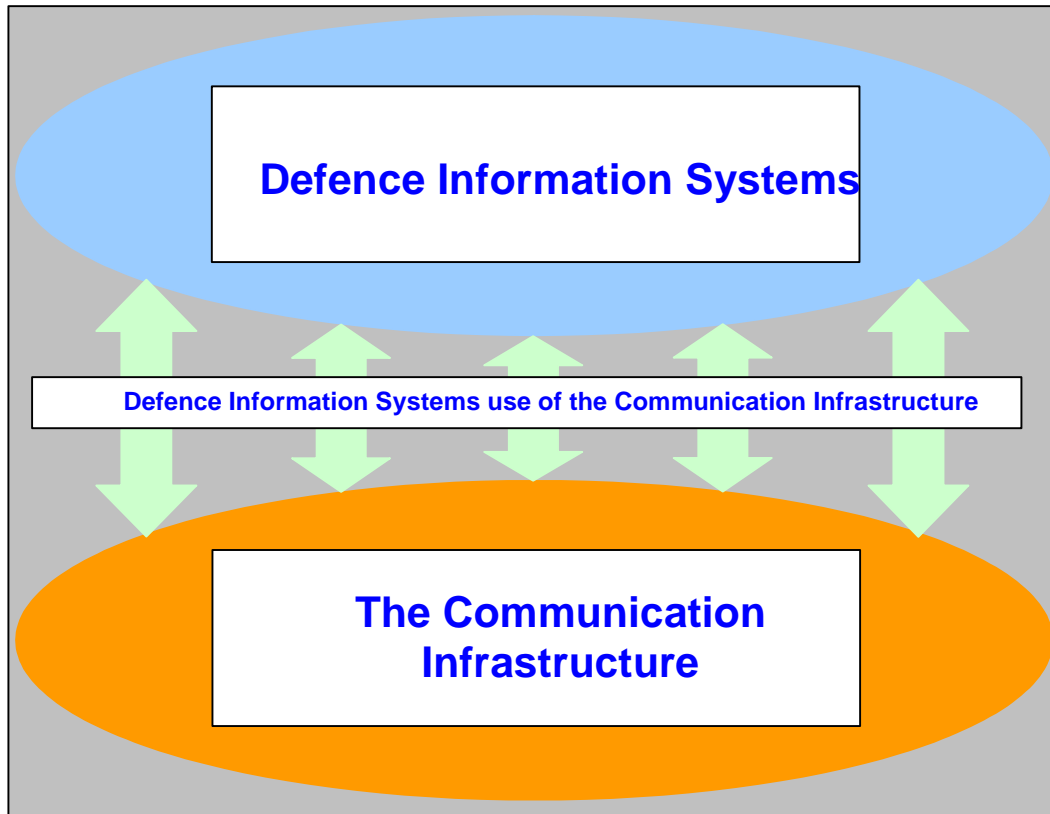


Figure 9-1: General Top-Level architecture

At the top-level, the information target architecture is described with three basic components:

- Military information systems and applications which reside at the application layer (~ layer 3) of the DEFCOMM reference model.
- The communication infrastructure with network and transmission mechanisms. This is transmission layer (~ layer 1) and convergence layer (~ layer 2) of the DEFCOMM reference model.
- Interface between the systems/applications and the communication infrastructure, thus making it possible for all military systems and applications to use the communication infrastructure for exchange of information. Related to the DEFCOMM reference model this interface is at the border between layers 3 and 2.

The general top-level architecture is illustrated in Figure 9-1.

The top-level architecture is not a layered approach, - the only purpose is to describe that the military systems and applications (information processing) are independent of the communication infrastructure (physical and logical communication) by using a well-defined and simplified interface. This architecture reflects the transition towards NBO, because the communication infrastructure architecture is separated from the application architecture.

9.1.2 IP Top Level

This section describes the *IP Top-Level* architectural view which is an aggregate of the IP-convergence architectural view (see section 5.2) and the general top-level architectural view (see section 9.1.1). Figure 9-2 illustrates in more detail the simplified interface when the IP-convergence architectural view is aggregated with the top-level architectural view.

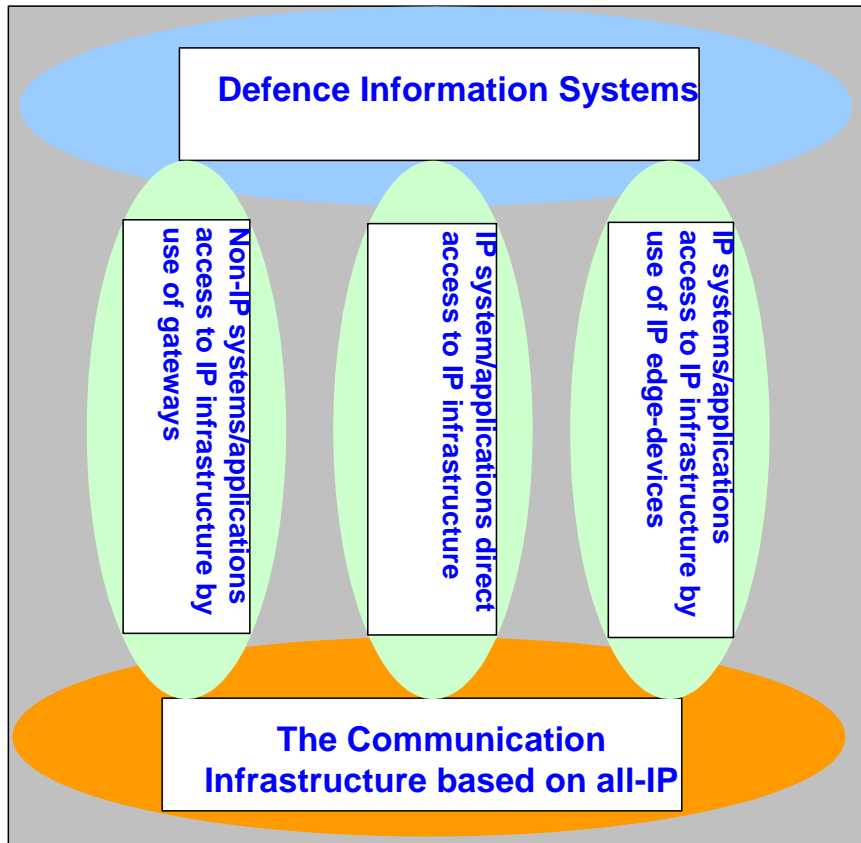


Figure 9-2: IP Top-Level Architecture

The three different ways of interfacing between the IP-based communication infrastructure and the military systems are:

- No interface. A direct connection means that native IP-based applications have direct access to the infrastructure by use of the IP-suite. This implies full network interoperability between applications; - however, the interoperability at higher levels must be ensured by the applications themselves. The network interoperability is also available to applications interfaced by gateways or edge-devices; however, this interoperability may be reduced by limited functionality of the gateway or edge-device.
- Gateway as interface. A gateway is used to translate information between a non-IP system/application and the IP-infrastructure. The functionality of the gateway is essential for the service integration between the non-IP and IP-systems. This type of gateway is described in more detail in the IP-convergence architectural view (see section 5.2).
- IP edge-device as interface. An IP edge-device is used for converting information at the IP-network level. The edge-device has a specific functionality

for communication to the IP-infrastructure. This can be a transparent functionality in both directions, eg a standard IP-router, - or it can be a firewall with filtering of the traffic. Another example is an edge-device for using the IP-infrastructure as a transmission network (~ a tunnel through the IP-infrastructure) without actually exchanging information, eg a VPN, a crypto-device, or a proprietary application.

These three ways can be mixed in hybrid interconnections.

It is important that the types of interfaces between the systems/applications and the communication infrastructure are very limited in order to separate the military systems/applications from the communication systems. Thus it is possible to describe the architecture of the communication infrastructure and the application architecture separately. This is done in sections 9.3 and 9.2 respectively.

The communication infrastructure based on all-IP (referring to Figure 9-2) consists of both the IP-network at the convergence layer and the transmission mechanisms (links, trunks, fibre, radios, etc) at the transmission layer of the DEFCOMM reference model.

9.2 Defence Information Systems

This section describes the military systems and applications from a top-level point of view.

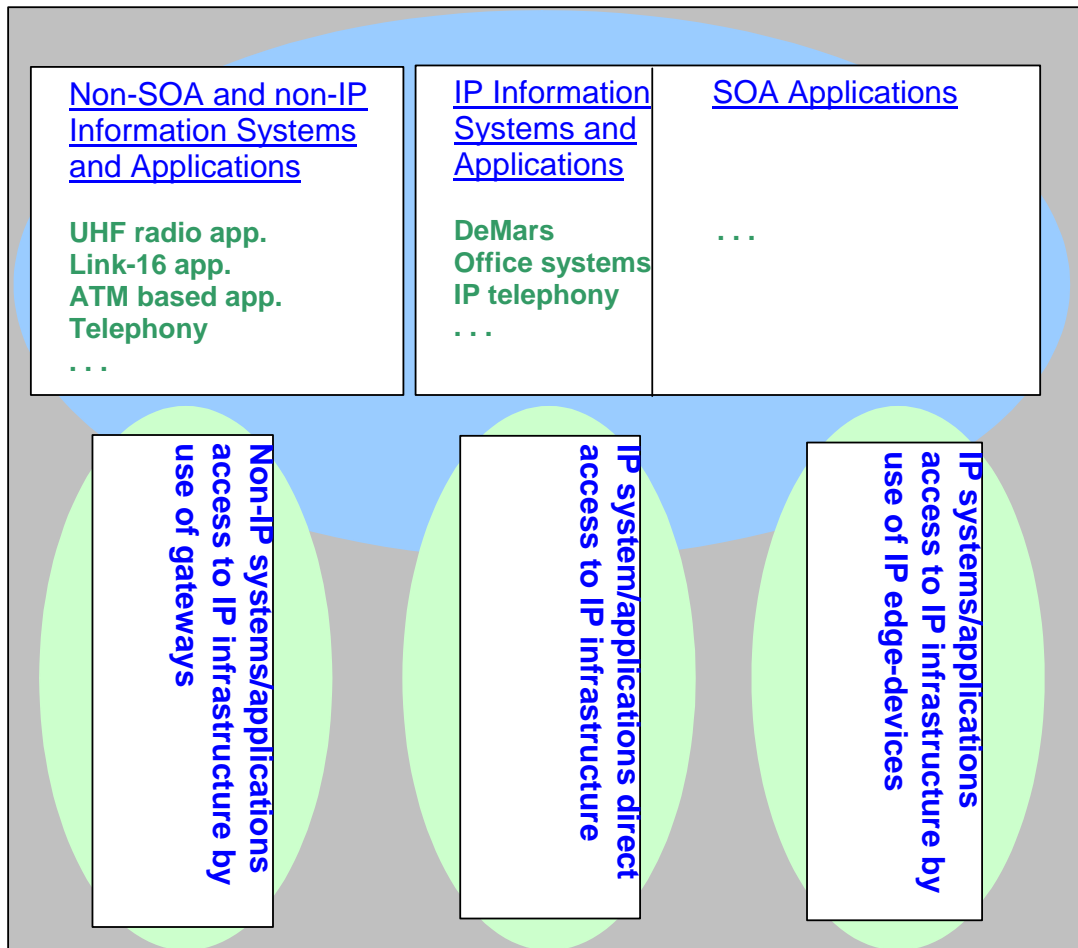


Figure 9-3: Application types interface to communication infrastructure

There are different types of applications according to the IP top-level architectural view, see section 9.1.2. The types of military systems and applications are illustrated in Figure 9-3. The figure illustrates that SOA applications are always IP-compliant because of the service integration (at the integration layer). All IP-compliant information systems and applications (including SOA applications) can access the IP-infrastructure either directly or by use of IP edge-devices. The figure also illustrates that all non-IP based information systems and applications must interface to the IP-infrastructure by use of gateways.

The three types of information systems and applications are dealt with separately in the subsequent three subsections.

9.2.1 Non-SOA and Non-IP Information Systems

It's outside the scope of this report to deal with the target architecture of non-IP information systems (including applications). Either these systems must operate autonomously or they must interface to the IP-infrastructure by use of an appropriate gateway. For interoperability this gateway must translate the non-IP information into IP-information – and vice versa.

9.2.2 IP-compliant Information Systems

IP-compliant information systems (including applications) can use the communication infrastructure with a homogeneous IP-convergence layer. The IP-convergence layer makes it possible to reach an arbitrary network device in all interconnected networks for all the systems, services, and applications available at the application layer of the DEFCOMM reference model.

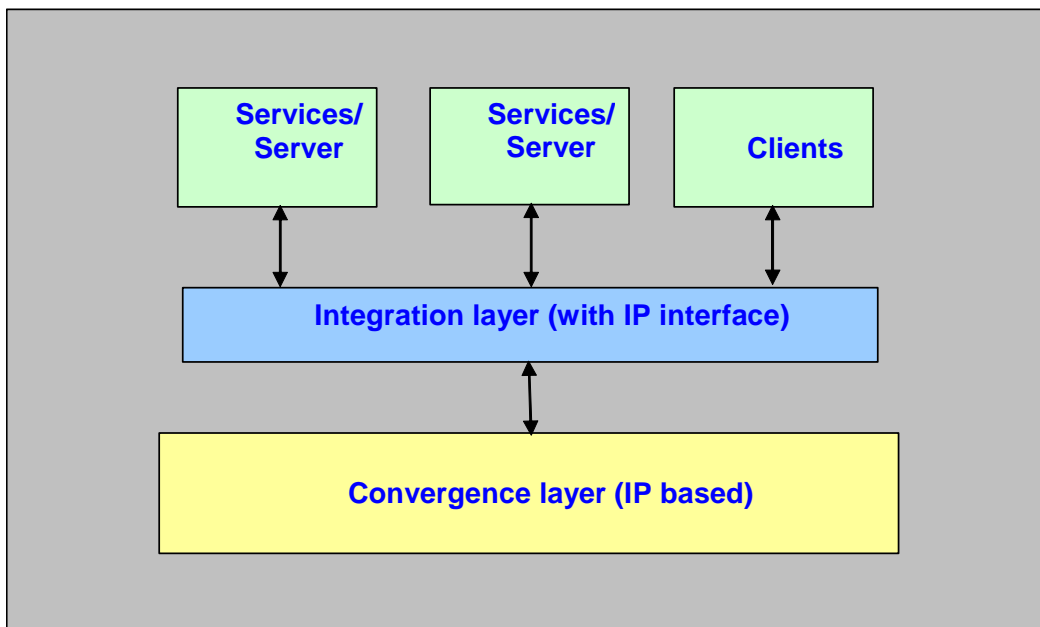


Figure 9-4: IP-applications with integration layer as interface to communication

The target architecture has full IP-compliance at the application layer for all applications using the IP-application protocols. For SOA applications this is accomplished by IP-interface protocols at the integration layer. This is illustrated in Figure 9-4.

9.2.3 SOA-based Information Systems

The top-level application architectural view shows how a combination of multi-tiered client/server systems and SOA can support future needs for operability at the application layer, - including NBO. SOA may serve as a unifying layer principle at the application layer. The target architecture of the applications will be a compromise between a high degree of interoperability and a relatively loose coupling between the

systems and application available. This is carried out by using a set of techniques and protocols enabling the semantic network at the application layer. The unified service is illustrated in Figure 9-5.

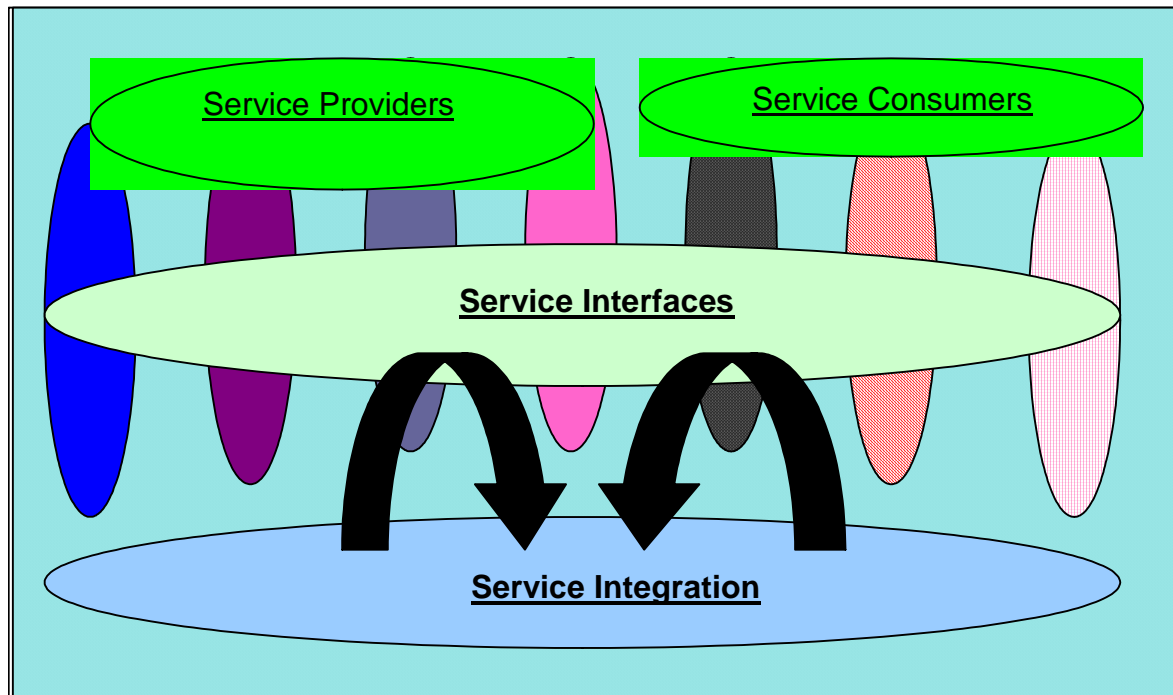


Figure 9-5: Unified service

The communication infrastructure is only a transport network for the applications, ie SOA based applications are separated from the communication infrastructure.

The loose coupling allows legacy systems to function and evolve autonomously – however, non-SOA applications may still exist in the target architecture.

9.3 The IP Communication Infrastructure

This section describes the IP communication infrastructure. It consists of a (large) number of networks connected by various transmission mechanisms. This forms a network of networks as described in section 9.3.1. The basics of one of these networks are described in section 9.3.2. In section 9.3.3 the IP-infrastructure is shown as an overlay network on all transmission mechanisms, and finally in section 9.3.4 the IP-infrastructure is shown as a fixed backbone network with the possibility of interconnecting other networks in a highly dynamic way.

These four architectural views make it possible to deploy a networked infrastructure according to the various tasks of the Danish Armed Forces as identified in [Ref. 1]. The properties of this infrastructure are described in more detail in the architectural views (see chapter 5), and some more specific references are given in the subsequent subsections.

9.3.1 The IP-Infrastructure as Networks of Networks

This section describes the communication infrastructure as IP-based networks of networks tied together with transmission mechanisms. This is illustrated in Figure 9-6 which also shows the interface to the defence systems and applications. The networks (with **orange** and **pink** colours) can be anything from a simple network with one network device to large networks of networks with thousands of network devices. The networks at the border (with **orange** colours) of the infrastructure contain access points to the defence systems and applications - either by gateway or edge-device interface, or directly connected. The transmission mechanisms are shown by the **black** lines between the networks.

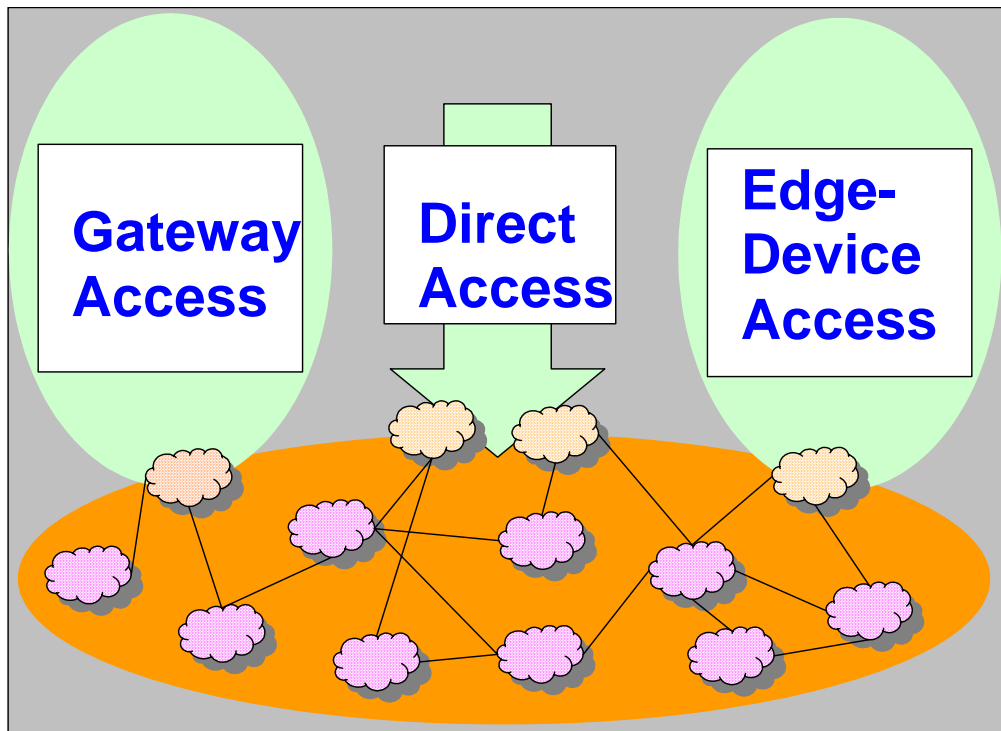


Figure 9-6: IP networks of networks

9.3.2 The basic network

This section describes the **basic network** as part of the communication infrastructure. In principle one network can consist of “networks of networks”, but a basic network as a simple building block is characterised by:

- The network transmission mechanism. Examples are LAN, WLAN, and Bluetooth.
- At least at Point-of-Presence (PoP), ie the possibility of communication to other similar networks. There are two types of PoP's:
 - Direct communication at the convergence layer. An example is a router.
 - Use of a transmission mechanism from the transmission layer. Examples are UHF radio network, satellite link, and fibre link.
- At least one network device, examples are hosts, sensors, or terminals.

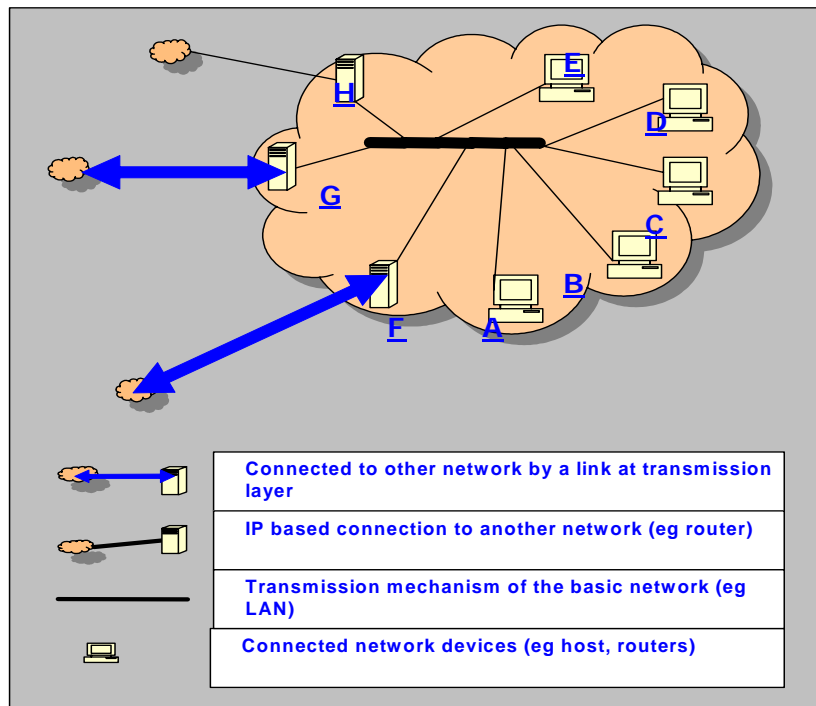


Figure 9-7: Example of a basic network as building block

Examples of these components are illustrated in Figure 9-7: The transmission mechanism is a LAN, network devices are A-E, and PoP's are F-H.

The basic network as a building block makes it possible to build a communication infrastructure of networks of networks supporting the tasks of the Danish Armed Forces. Most of the architectural view described in chapter 5, - including local, regional, and global subsystems, universal, security, E2E, and mobility - is comprised of these basic networks. This applies to the top-level architectural view within this chapter as well.

The major part of the PoP's should be at the convergence level. However, the PoP's at the transmission layer are needed for use of specific military transmission mechanisms, - this is further elaborated in section 9.3.3.

Though this basic network view is protocol independent, it is assumed that IP is the convergence protocol

9.3.3 The IP-Infrastructure with the Transmission Mechanisms

This section describes the important aspect of making the convergence layer a kind of overlay network on all transmission mechanisms. Figure 9-8 illustrates how the IP as an overlay gathers all transmission mechanisms.

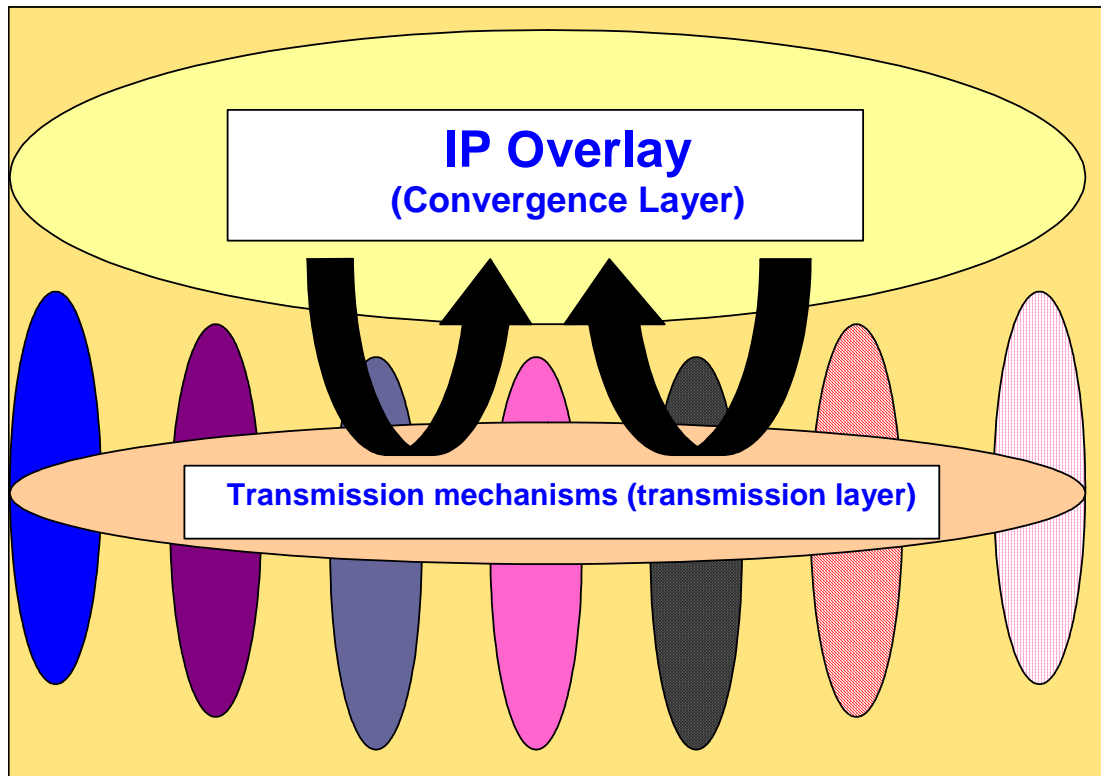


Figure 9-8: Convergence as overlay on all transmission mechanism

With IP as the chosen convergence protocol the basic components¹⁰ at the IP-convergence layer will be COTS, ie civilian technology. Many transmission mechanisms may be COTS as well, but specific requirements for military communication should be handled by robust transmission mechanisms at the transmission layer.

This means that the IP-infrastructure uses all different mechanisms available for a specific task, - this includes ATM networks, PSTN/ISDN, SATCOM, MPLS networks, UHF, VHF, HF, fibre, ethernet, Bluetooth, Internet, or TDL's. The information and the application (with operational requirements) will determine which transmission mechanism(s) to use. Requirements like security, QoS and capacity determine the mechanism to be used, thereby referring back to most architectural views in chapter 5, including local, regional and global subsystems, QoS, security, E2E, and mobility. The architectural view fitting all this together is the network management architectural view.

9.3.4 The IP-Backbone and the Dynamic Infrastructure

The purpose of this section is to describe the IP-infrastructure as a static and a dynamic infrastructure.

¹⁰ Specific military components may be included in the civilian architecture, ex. military cryptography in IPSec. However, IPSec is regarded as the basic component in this context.

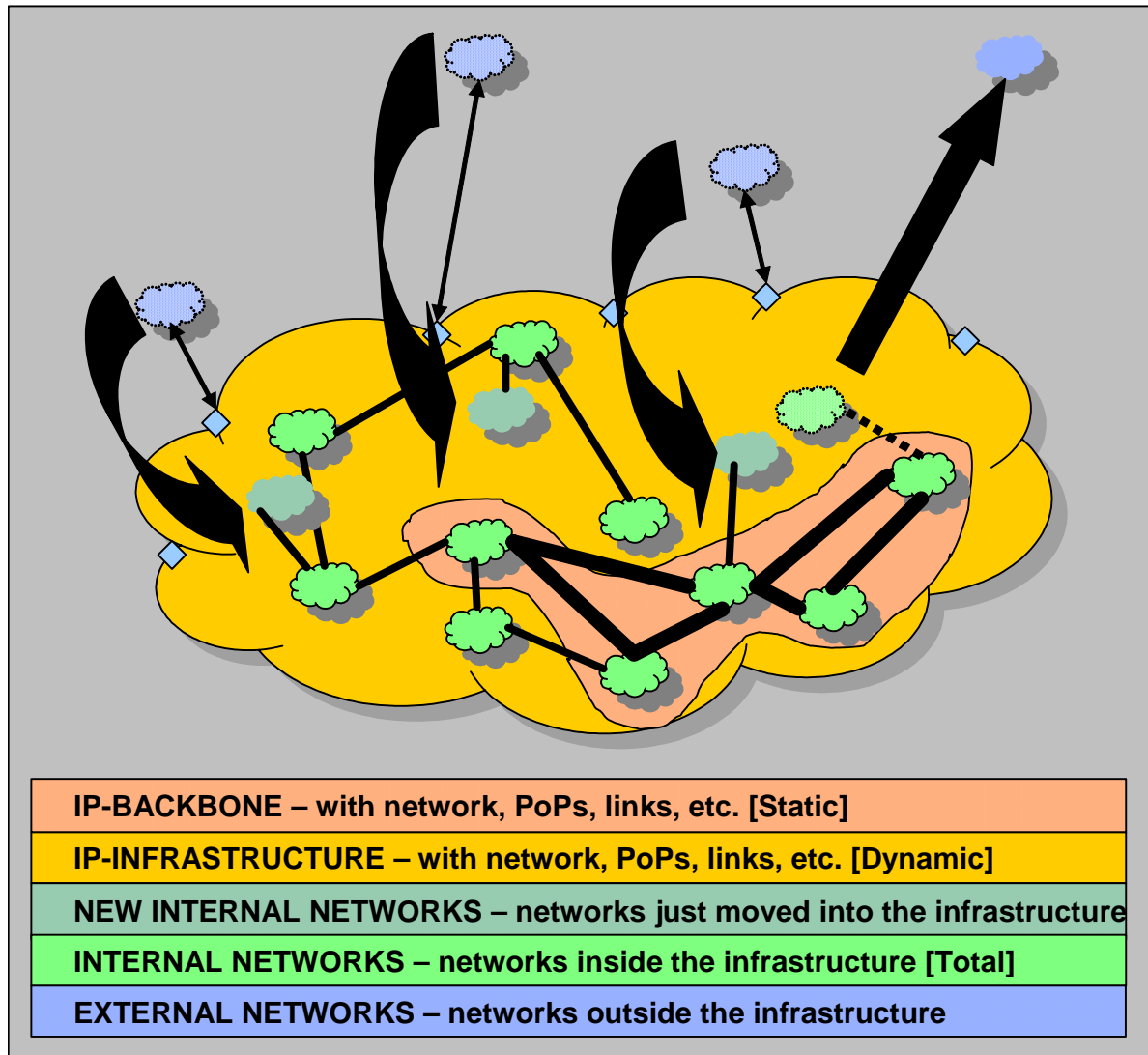


Figure 9-9: Example with IP-backbone and dynamic infrastructure

The target architecture thus consists of:

- The **static IP-infrastructure**, - also denoted the **IP-backbone**. The IP-backbone is kept as the principal and permanent part of the IP-infrastructure. The IP-backbone must always be available (~ operational) and thus the basis (~ backbone) for the remaining part of the infrastructure. The IP-backbone can be defined from operational, technical, political, or other reasons. However, the main purpose is to have a basic and fixed communication infrastructure making it possible for the Armed Forces to establish the needed networks to accomplish the tasks. Though the IP-backbone is a static environment it may be changed over time; however, changes should occur rarely. In Figure 9-9 the backbone is illustrated by the *orange* colour.
- The **dynamic IP-infrastructure** is the part of the infrastructure which can be dynamically extended or reduced from the actual operational situation, - including short specific tasks. In principle, this part of the IP-infrastructure can be changed any second. In Figure 9-9 the dynamic infrastructure is illustrated by all networks outside the yellow area. Some networks are not (yet) part of

the infrastructure, ie stand-alone networks. Networks being connected may be fixed networks built on a local infrastructure or they can be mobile ad-hoc networks built without a fixed infrastructure.

Thus the total IP-infrastructure is made up of a (large) number of networks which in a dynamic way can be connected or disconnected. This is supported by the mobility architectural view (see section 5.11). In Figure 9-9 this is illustrated with a snapshot of the IP-infrastructure, including PoP's (marked as blue rhombs in the figure). The total IP-infrastructure will change when networks are connected and disconnected.

This dynamic infrastructure supports most of the architectural views in chapter 5, - including E2E, NBO, security, global information network, and local, regional, and global subsystems. However, the dynamic infrastructure is a big challenge to the network management architectural view.

Further details on the IP-infrastructure and interfaces to the transmission layer may be found in the IP-convergence architectural view (see section 5.2) and the basic network (see section 9.3.2).

The needed flexibility of the dynamic IP-infrastructure requires that a unified IP-backbone is available, and it is important to ensure this backbone is deeply rooted in fixed military and civil networks.

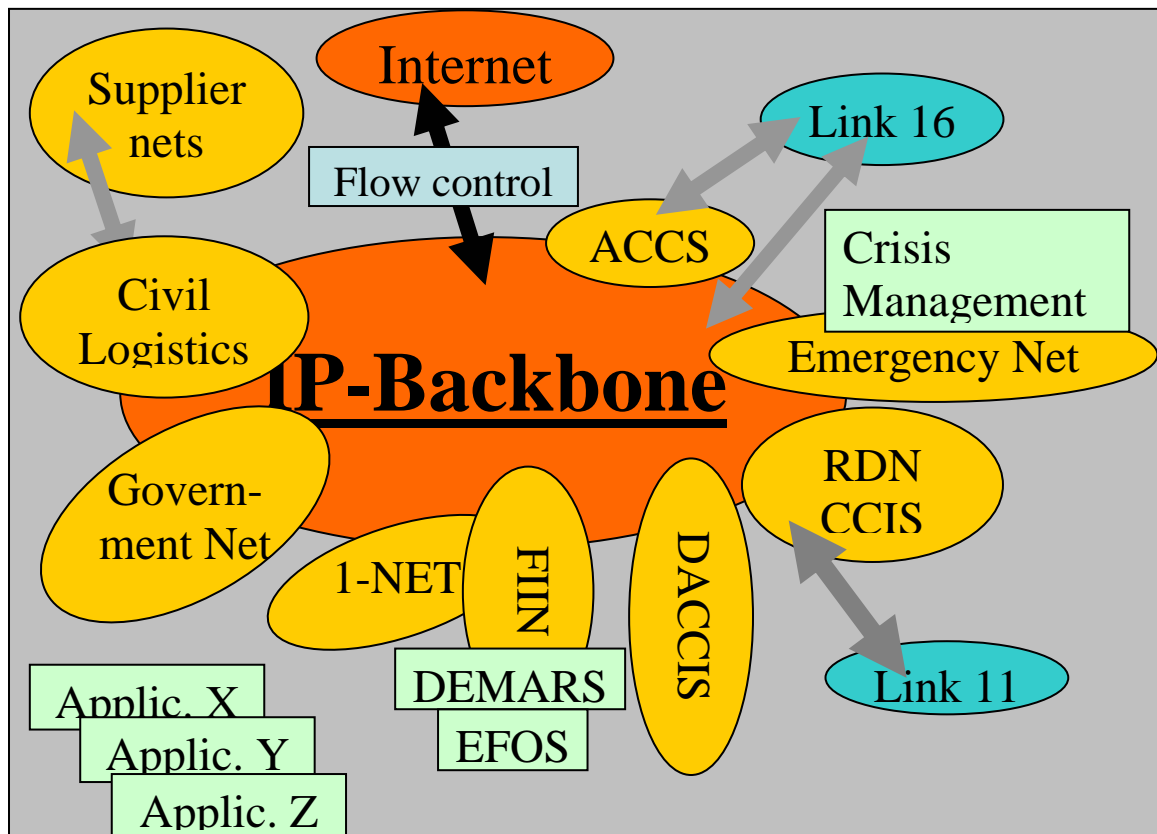


Figure 9-10: Example of IP-backbone based on current networks

9.3.4.1 Example of on IP-backbone

In this section an example of an IP-backbone based on current or planned networks is described.

Figure 9-10 illustrates how the backbone can be build from current networks like ACCS, RDN CCIS, DACCIS, the planned 1-NET, etc. It should be noted that only the IP-part of these networks may be part of the IP-infrastructure, - furthermore only the static part may be interconnected as part of the IP-backbone. In this example, the IP-backbone consists of parts of different existing or planned networks, which are in accordance with evolutionary architectural views (see sections 5.9 and 5.10).

In this example, the Link 16 systems are regarded as autonomous non-IP systems. This requires a gateway to access the IP-backbone.

For availability reasons this IP-backbone must be robust for all services, ie a physical or logical segmentation of the backbone should be considered. In Figure 9-11, it is illustrated how current military systems can be connected to the IP-infrastructure through different backbone segments based on the operational use of the networks.

The flow controls between the backbone segments and the Internet are related to the security architectural view (see section 5.5).

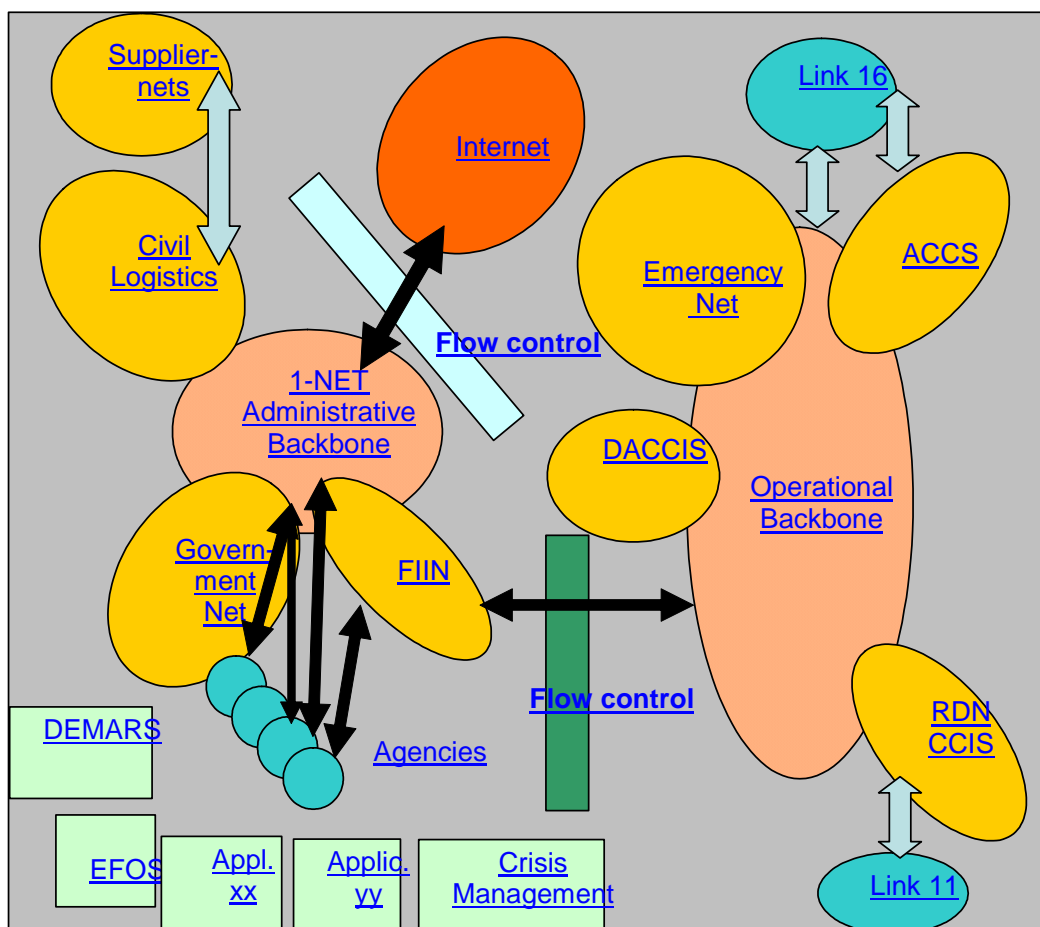


Figure 9-11: Example of IP-backbone segmentation

9.3.5 Concluding Remarks on the Top-Level Target Architecture

The target architecture is formed by a military information systems and a communication infrastructure with a static and a dynamic part. To facilitate the evolutions towards SOA and converged network of networks, only a limited number of types of interfaces must exist between the information systems and the communication infrastructure. For communication flexibility, the IP-infrastructure must be divided into a static and a dynamic infrastructure, and the robust system architecture of the static part (ie the IP-backbone) may be developed from existing military and civil IP-based networks.

10 Conclusions and recommendations

This chapter summarizes the conclusions and recommendations from the main body of the report. The recommendations have been grouped into *communication and network* aspects, *evolution* issues, and matters concerning the *integration of applications*.

From a technical point of view it is possible to integrate most of the military and total defence (~ homeland security) networks into a network of networks by use of the Internet Protocol (IP) as convergence protocol. Convergence at the application level can be achieved by use of a Service Oriented Architecture (SOA). The converged network based on IP and applications based on SOA are the cornerstone of the target architecture.

This report (WP3) is focused on the technological and technical aspects of the transition towards NBO. It must, however, be emphasized that doctrinal, organizational and cultural aspects in the process are at least as important, and must in depth be dealt with elsewhere.

10.1 Recommendations Concerning Architectures and Evolution

The target architecture including all the presented architectural views should be used as guidance for planning, acquisition, and the maintenance process for ICT systems. This includes the development and maintenance of system architectures – detailed instantiations of the target architecture with available technology and standards.

The ICT aspects must be assessed for all NBO related acquisition, including all sensors and effectors to make sure that they fit into the overall architecture.

It is recommended to use a staged approach, where a number of well-defined milestones manage the development into an overall network of networks with a loose coupling between component systems. The final goal is to integrate all networks and applications into the overall scheme, although some services and functionalities are yet to be fully supported due to lack of the needed technology.

Make adherence to the general principles mandatory. Stove piped systems should cease to exist. Legacy systems may be integrated by wrapping, i.e. providing SOA interfaces to them.

The proposed architectural guidelines are in accordance with the anticipated coalition partners, and should remain so. NATO and other international studies such as NNEC Feasibility Study, TACOM Post 2000, and MIP are examples of current studies to follow.

Conduct experiments to demonstrate use, advantages, and technological feasibility of the principles. This may involve Danish or other relevant industry in partnering ventures to conduct CDE. It is strongly recommended that COTS technology should not be implemented before it has reached a mature state.

10.2 Communication and Networks

To obtain interoperability at the network level, it is recommended to use the IP as the protocol for the converged network infrastructure. This converged network infrastructure should be made up of an IP-backbone as the principal part and a dynamic IP-infrastructure as a flexible part used for (short) specific tasks.

The evolutionary and staged approach means that the acquisition processes must include an assessment of the IP-capabilities of the communication equipment, including effectiveness of IP-interfaces and aspects of QoS, security, management, etc.

Groups of networks such as administrative and operational networks may at least for some time have to be separated by information flow devices for security reasons. To limit damage from failure or intrusion incidents the total network must be segmented, logically or physically.

To fully exploit the network of networks concept, a global and integrated directory service and naming scheme for the total network of networks should be available.

Apply unified network management wherever possible. This requires agreed management standards to be defined, and all relevant networks and network components must adhere to those standards. SNMP is an example of such a standard.

Many networks already use the IP-suite, but it may be necessary to use gateways to connect some of the legacy networks to the global network.

As the first step it is recommended to develop the system architecture for a unified IP-based backbone as basis for a flexible and dynamic communication infrastructure. This IP-backbone may include relevant existing IP-based networks. The IP-part of FIIN is highly relevant, but 1-NET and operational networks based on IP should be considered as well. Also the integration of other legacy networks and systems into the joint IP-backbone has to be considered.

10.3 Integration of Applications

To obtain flexibility and loose coupling between component systems, it is recommended to use a SOA as the overall architectural principle.

It is important that the armed forces obtain and keep a high level of knowledge of SOA, and that this knowledge is broadly available.

It is strongly recommended to exploit the loose coupling inherent in SOA to let the different systems (services and service consumers) evolve at their own pace. This includes applications, tactical networks and other dedicated networks.

Work towards semantic interoperability by using a common joint data model such as JC3IEDM, supplemented with ontologies.

As the first step it is recommended to develop measures based on simple metrics to evaluate the degree of network readiness of all relevant present and future systems and components. Use the methods in the acquisition process.

10.4 Caveats

It must be emphasised that the recommendations above are not without a cost. Important points to consider are:

- For the time being IP has no mechanism for meeting hard real time requirements.
- SOA implemented as web-services imposes a substantial overhead, leading to additional load on communication channels and on computer nodes.
- The adherence to the general architectural principles may constrain the choice of technologies, acquisition practices and introduction of new systems.

References

- Ref. 1: DEFCOMM, Operational Scenarios, WP1, DDRE report M-17/2005 (Sep 2005).
- Ref. 2: DEFCOMM, Requirements to Information in Network Based Operations, WP2, DDRE report M-18/2005 (Sep 2005).
- Ref. 3: Rapport fra Ministeriet for Videnskab, Teknologi og Udvikling om Mulige Fællesoffentlige Arkitekturkrav, 10 december 2004, version 1.21. (Danish)
- Ref. 4: NATO Network Enabled Capability (NNEC) Study vol. 2, NC3A JUL 2005.
- Ref. 5: Koordinationsgruppen vedr. Netværksbaserede Operationer, Indledende Rapport, FAK 21 DEC 2004 (Danish).
- Ref. 6: HKOM, HRN Kommunikation, Målarkitekturen, WP3 af HKOM projektet, FOFT M-10/2005 (Danish)
- Ref. 7: NATO Architecture Framework (NAF), Enclosure to EAPC(AC/322-SC/2-WG/4)WP(2003)002-Rev1, dated 7 October 2003).
- Ref. 8: DOD Architecture Framework 1.0, 9 February 2004.
- Ref. 9: Ni Noter om Netværksbaseret Forsvar, Forsvarets Högskola 2005.
- Ref. 10: NATO C3 Technical Architecture, ver. 6. SEP 2004, NOSWG.
- Ref. 11: Net-Centric Operations and Warfare (NCOW) Reference Model (RM) Version 1.1 (v1.1) Draft, DOD OCT 2004.
- Ref. 12: TACOMS Post 2000, Final Study Report Annex 1: Architecture Overview, TacOne Sept. 2002. – TACOMS Post 2000 to be published as STANAG 4637-4647.
- Ref. 13: Anthony W. Isenor: A Brief Assessment of LC2IEDM, MIST and Web Services for use in Naval Tactical Data Management, DRD Canada 2004.
- Ref. 14: Hvidbog om IT arkitektur (Whitebook on IT Architectures), Ministeriet for Videnskab, Teknologi og Udvikling 2004 (Danish).
- Ref. 15: Delstudie om Teknologi og Standarder (Study on Technology and Standards), CHOD DEN CCIS 2004.
- Ref. 16: Udkast til delstudie om Interoperabilitet (Draft Study on Interoperability), CHOD DEN CCIS 2004 (Danish)
- Ref. 17: Network Enabled Capability, Unified Message 1. draft, UK MOD SEP 2004.

- Ref. 18: Information Superiority Nato Network Enabled Capability Integrated Project Team (IS-NNEC IPT) Interim Strategic Vision and Concept for NNEC, SACT July 2004
- Ref. 19: Netværksbaserede Operationer i Flyvevåbnet, AG/NBO/FLV, OCT 2004 (Danish).
- Ref. 20: Udkast til Hærens strategi for netværksbaserede operationer, HOK, AG/NBO/HRN SEP 2004 (Danish).
- Ref. 21: Teknologisk Udvikling af Betydning for C2CS, DDRE Report M-08/2004 (Danish). Basis for Ref. 15.
- Ref. 22: MIP JC3IEDM Edition 0.6, MIP Data Modelling Group 2005. [MIP C2IEDM Edition 6.1.5b, MIP Data Modelling Group 2004]
- Ref. 23: Link 16 i Forsvaret (Link 16 Study), DDRE M-12/2005 (Danish).
- Ref. 24: Operational Concepts for the Secure Communications Interoperability Protocol (SCIP), AC/322(SC/1)WP(2005)0002.
- Ref. 25: Enterprise SOA, Dirk Krafcig, Karl Banke and Dirk Slama, Prentice Hall, Pearson Education, 2005.
- Ref. 26: Position Paper by NATO/RTO/IST Task Group on Network Enabled Capability Security, Oct 2004 (to be published).
- Ref. 27: ISO/IEC TR 9575, the OSI Routing Framework.

Appendix A: Enabling Technologies for Network Management

In this appendix, a set of enabling technologies and protocols that are commonly recognized to be potential candidates for intelligent distributed network management will briefly be presented.

Policy-based Network Management

In policy-based network management, policies are defined as rules that govern the states and behavior of the network system. The most significant benefit of policy-based network management is that it promotes the automation of establishing management level objectives over a wide-range of network devices. Network administrator would interact with the network by providing high-level abstract policies which are device independent and human-friendly and which are automatically translated to low-level device-dependent configurations derived from the high-level policies. Policy-based NM can adapt rapidly to changing management requirements via run-time reconfigurations, rather than re-engineer new object modules for deployment which is also an attractive solution for large networks with frequent changes in operational directives. IETF's Resource Allocation Protocol (RAP) plays a key role in policy-based network.

Distributed Object Computing

Distributed Object Computing (DOC) uses Object-Oriented (OO) methodology to construct distributed applications. Its adaptation to network management is aimed at providing support for distributed network management architecture, integration with existing heterogeneous network management solutions and providing development tools for distributed network management components. DOC provides distribution of services and applications in a seamless and location transparent way, by separating object distribution complexity from network management functionality concerns. Two major adaptations of DOC to network management are:

- Common Object Request Broker Architecture (CORBA)
- Distributed COM (DCOM)

Web-service based NM

Web technology would influence NM only to some degree. With respect to NM, the critical problems Web-service based NM tries to address are:

- Platform heterogeneity. Traditional NM solutions are highly platform-dependent.
- Lack of management console accessibility. Network administrators must operate on proprietary management consoles to perform their operations, and the user interfaces for each management platform may vary significantly. Web technology effectively addresses this problem by providing ubiquitous management consoles in the form of standard web browsers.
- High cost of management platform deployment and maintenance.

Web technology does not implement a distributed paradigm in NM. The burden of implementing distribution is largely left to higher-level management architecture. In general, web-based technology is better used for providing web access to managed devices, especially if the user of the management application does not have much domain specific knowledge.

Web technology is provided by HyperText Markup Language (HTML), eXtensible Markup Language (XML) and Java applet in information presentation, providing a seamless Graphic User Interface (GUI) accessible everywhere.

Code Mobility for Network Management

Code mobility can be considered the capability of an application to distribute and relocate its components at run-time. This can be achieved by dynamically transporting programmes from managers to agents and performing the delegated management tasks locally.

With code mobility, management tasks no longer have to be performed by the managers. They simply generate management objectives and outline task procedures. The execution of tasks is delegated to the agents. Code mobility is not a good candidate for networks with simple but frequent service requests.

Intelligent Agents

An intelligent agent is an independent entity capable of performing complex actions and resolving management problems on its own.

Unlike code mobility, an intelligent agent does not need to be given task instructions to function, rather just the high-level objectives. The use of intelligent agents completely negates the need for dedicated manager entities; as intelligent agents can perform the network management tasks in a distributed and coordinated fashion, via inter agent communications.

Many researchers believe intelligent agents are the future of network management, since there are quite some significant advantages in using intelligent agents for network management.

Intelligent agents may provide a fully scalable data processing and decision-making capability. They are completely distributed, which alleviates management bottlenecks as seen in centralized network management solutions. In this way the resulting network management system is more robust and fault tolerant, as the malfunction of a small number of agents will have no significant impact on the overall management function.

As the entire network management system is autonomous, network administrators will only need to provide service-level directives to the system.

The intelligent agents are self-configuring, self-managing, and self-motivating. Such a system would largely ease the burden of NM routines that a network administrator has to currently struggle with.

However, the application of an intelligent agent is still at its infancy, and many difficult issues still remain unsolved.

Active Networks

Active network is considered a new approach to network architecture in which the network nodes, such as routers and switches, perform customized computation on messages flowing through them. In active networks, routers and switches run customized services that are uploaded dynamically from remote servers or via code mobility.

Active networks, combined with code mobility, present an effective enabling technology for distributing management tasks to device level.

NM based on economic models

Network management using economic theory proposes to model network services as an open market model. The resulting network is self-regulating and self-adjusting, without the presence of any formal network management infrastructure. Network administrators would indirectly control the network dynamics by inducing incentives and defining aggregate economic policies. Using economic models for managing multi-agent systems could be a viable alternative, due to its simplicity and self-sustaining nature.

Appendix B: Web-Services in Perspective

This appendix gives a brief discussion of advantages and disadvantages of Web-Services as they have been implemented recently. The discussion is based on [Ref. 13] and deals with the following points:

- Vendors, ie what is the supply situation for the technology?
- Cost, ie what is the cost by purchase and wide spread use of the technology?
- Openness, ie are there implementations based on open, non proprietary standards?
- Maturity, ie at which development stage is the technology?
- Evolution potential, i.e. does the technology seem to be promising in the sense that it may be an important vehicle for NBO in Denmark?

1. *Vendors*

The specifications for the Universal Description and Discovery Interface (UDDI) are published and maintained by the W3 consortium. The same applies to the Web Services Description Language (WSDL), and also the Simple Object Access Protocol (SOAP) and XML standards are public. Many vendors, including Microsoft and IBM support these specifications in their products. One example is the Microsoft .NET philosophy and product suite. In the Danish arena a number of software houses also adhere to these open standards. It is thus possible to implement web services and avoid a single source situation.

2. *Cost*

Implementing Web services in it self does not necessarily cost anything, in the sense that development tools are available and efficient. The complexity of Web services compared to simpler client/server implementations will however add both to the development costs and to the requirements for computer power and transmission capacity.

3. *Openness*

Web Services standards are open and easily available. It should, however, be noted, that even if the standards are followed, the different vendors of development tools differ in their application of the standards. This is particularly the case for the implementation of the UDDI mechanism.

4. *Maturity*

SOAP, WSDL and UDDI represent the core technologies of Web Services. The first UDDI schema specification was created in 1999. The SOAP specification was first introduced in early 2000. Finally, the first working draft of the WSDL specification was in April 2002. The specifications are now relatively stable, but should still be considered relatively immature technologies. The UDDI mechanism is relatively complicated and therefore differently implemented by different vendors. So even if it does work, it is still relatively immature.

5. *Evolution Potential*

Web services have the potential of forming a general convergence layer for applications, including service consumers, in a networked environment. It is thus one possible technology for forming the basis for NBO in Denmark. Because of its dependence on the Internet Protocols, and because of the service orientation, there are still some shortcomings, such as real time performance and security. Many sources, including [Ref. 12] and [Ref. 13] believe that SOA and especially Web services will be the mainstream technology of the next decade.

6. *Overall Assessment from a Tactical Data Perspective*

Web Services provide the capability of separating applications into functional components, developing those components on different platforms, using different languages, and deploying them at different sites. In terms of the management of tactical data on a single asset (eg, a submarine), Web Services provide the ability to integrate disparate tactical systems. This may be applied to legacy components of a tactical system. The concept of a web service wrapper, placed around a legacy system, would open the system to all other web service systems on the local asset. In this regard, Web Services may be useful when integrating existing disparate tactical systems. For any new developments involving the integration of multiple tactical systems (ie, a combat system), it is unlikely that Web Services would play a part. This is primarily because the problems that Web Services were developed to address (ie, unknown hardware, unknown software languages and unknown interfaces) are not present.

Acronyms

1-NET	One network for classified and unclassified information
ACCS	Air Command & Control System
ATCCIS	Army Tactical Command & Control Information System
ATM	Asynchronous Transfer Mode
BC	Boundary Control
BDE	Brigade
BLOS	Beyond Line Of Sight
BMS	Battle Management System
C2	Command & Control
C4ISR	Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance
CA	Certificate Authority
CBIS	Content Based Information Security
CCIS	Command & Control Information System
CDE	Concept Development & Experimentation
CIDR	Classless Interdomain Routing
COM	Component Object Model
COP	Common Operational Picture
CORBA	Common Object Request Broker Architecture
COTS	Commercial of-the-shelf
DACCIS	Danish Army Command & Control System
DEFCOMM	Danish Defence Communication
DEM	Data Exchange Mechanism
DeMars	Danish Defence Management and Resource System
DEOS	Danish Army Communication Network
DIV	Division
DAP	Directory Access Protocol
DCOM	Distributed COM
DDRE	Danish Defence Research Establishment
DOC	Distributed Object Computing
DOD	Department of Defense
DoS	Denial-of-Service
DSML	Directory Service Markup Language
E2E	End-To-End
EbXML	e-busines XML
EFOS	Etablissement FORvaltnings System (Danish)
FIIN	Danish Integrated Information Network
FTP	File Transfer Protocol
GIG	Global Information Grid
GMPLS	Generalized MPLS
GSM	Global System for Mobile communication
GW	Gateway
HAIPES	High-Assurance-IP-Encryptors
HF	High Frequency
HQ	Headquarters
HTTP	Hyper Text Transfer Protocol
HW	Hardware

ISO	International Standardization Organisation
ICT	Information and Communication Technology
IER	Information Exchange Requirements
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet security protocol
IPv4	IP version 4
IPv6	IP version 6
IS-IS	Intermediate-System-to-Intermediate-System
ISDN	Integrated Services Digital Network
IT	Information Technology
ITU	International Telecommunication Union
J2EE	Java 2 platform Enterprise Edition (Java EE)
JC2IEDM	Joint C2 Information Exchange Data Model
JC3IEDM	Joint C3 Information Exchange Data Model
JMS	Java Message System
JTA	Joint Technical Architecture
LAN	Local Area Network
LAS	Local Area Subsystem
LDAP	Lightweight DAP
LDIF	LDAP Data Interchange Format
LOH	Line OverHead
LOS	Line of Sight
LF	Low Frequency
LRG	Local, Regional, Global (sub systems)
MANET	Mobile Ad-hoc wireless NETworks
MEM	Message Exchange Mechanism
MIB	Management Information Base
MIDS	Multifunction Information Distribution System
MIP	Multilateral Interoperability Programme
MIP	Mobile Internet Protocol
MPLS	Multi Protocol Label Switching
MS	Mobile Subsystem
MTI	Moving Target Indicators
NAF	NATO Architectural Framework
NAT	Network Address Translation
NBO	Network Based Operations
NC3TA	NATO C3 Technical Architecture
NDAC	NATO Data Administration Group
NEC	Network Enabled Capability
NECCIS	Northern Europe Command and Communication Information system
NECSec	NEC Security
NGO	Non-Government Organisation
NI	Network Interface
NIS	Network Information Service
NIS+	Network Information Service Plus
NM	Network Management
NNEC	NATO Network Enabled Capability

NOSWG	NATO Open System Working Group
NS	Network Services
QoS	Quality of Service
OO	Object Oriented
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PAN	Personal Area Network
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
POH	Path OverHead
PoP	Point of Presence
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Network
RDNCCIS	Royal Danish Navy Command and Communication Information System
RF	Radio Frequency
RMON	Remote Network Monitor
RSVP	Resource ReSerVation Protocol
RTP	Real Time Protocol
RTO	(NATO) Research and Technology Organisation
SATCOM	Satellite Communication
SDH	Synchronous Digital Hierarchy
SDR	Software Defined Radio
SLA	Service Level Agreement
SLIP	Serial Line Internet Protocol
SMTP	Simple Mail transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOH	Section OverHead
SONET	Synchronous Optical NETwork
STS-XX	Synchronous Transfer Signal (signalling rate XX = 1, 3, 12,)
SW	Software
TA	Target Architecture
TACOMS	Tactical Communication
TBCE	Type B Cost Estimate
TCP	Transmission Control Protocol
TDL	Tactical Datalink
Telco	Telephone Company
TETRA	Terrestrial Trunked Radio
TM	Telecommunication Management
TMN	Telecommunication Management Network
TP2K	TACOMS Post 2000
UDDI	Universal Description, Discovery & Integration
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UMTS	Universal Mobile Telephone System
VHF	Very High Frequency
VMF	Variable Message Format
VoIP	Voice over IP

VPN	Virtual Private Network
WAS	Wide Area Subsystem
WEAO	Western European Armaments Organisation
Wi-Fi	Wireless Fidelity– Wireless LAN
WLAN	Wireless LAN
WPn	Work Package n
WS-BPEL	Web Services Business Process Execution Language
WS-CDL	Web Services Choreography Description Language
WSDL	Web Service Description Language
WWW	World Wide Web
XML	eXtensible Markup Language