FFI RAPPORT

NETWORK ARCHITECTURE FOR NETWORK CENTRIC WARFARE OPERATIONS

KURE Øivind, SORTEBERG Ingvild

FFI/RAPPORT- 2004/01561

NETWORK ARCHITECTURE FOR NETWORK CENTRIC WARFARE OPERATIONS

KURE Øivind, SORTEBERG Ingvild.

FFI/RAPPORT- 2004/01561

FORSVARETS FORSKNINGSINSTITUTT
Norwegian Defence Research Establishment
P O Box 25, NO-2027 Kjeller, Norway

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Norwegian Defence Research Establishment

P O BOX 25
N0-2027 KJELLER, NORWAY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

REPORT DOCUMENTATION PAGE

1) PUBL/REPORT NUMBER	2) SECURITY CLASSIFICATION	3) NUMBER OF PAGES
FFI/RAPPORT- 2004/01561	UNCLASSIFIED	79
1a) PROJECT REFERENCE	**2a) DECLASSIFICATION/DOWNGRADING SCHEDULE**	
FFIE/869/110	-	

4) TITLE

NETWORK ARCHITECTURE FOR NETWORK CENTRIC WARFARE OPERATIONS

5) NAMES OF AUTHOR(S) IN FULL (surname first)

KURE Øivind, SORTEBERG Ingvild

6) DISTRIBUTION STATEMENT

Approved for public release. Distribution unlimited. (Offentlig tilgjengelig)

7) INDEXING TERMS

IN ENGLISH:	IN NORWEGIAN:
a) Network Centric Warfare (NCW)	a) Nettverks basert forsvar (NbF)
b) Communication architecture	b) Kommunikasjonsarkitektur
c) IP	c) IP
d) COTS technology	d) COTS teknologi
e)	e)

THESAURUS REFERENCE:

8) ABSTRACT

This report is a delivery from the NBF-Grid project at FFI (Forsvarets Forskningsinstitutt).

The scope of this report is to roughly describe the mechanisms and functions required in a network architecture suited for the network centric warfare (NCW) concept. The focus is on the network services required to offer a robust, scalable and flexible network topology and architecture. The report does not describe applications, services and data definitions. However, it identifies the network components required to support both existing and future applications and services. Security architecture and services are not a part of the report and they will be analysed in a separate analysis.

Currently, all the NCW requirements cannot be fully met with the available technology and substantial further research is required. We have tried to identify the maturity of the areas. In particular we try to highlight the areas where military requirements substantially diverge from commercial requirements and where COTS (Common Off The Shelf) products are not sufficient, but specialized military solutions must be developed.

9) DATE	AUTHORIZED BY This page only	POSITION
3. January 2004	Vidar S Andersen	Director

ISBN-82-464-861-5

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

CONTENTS

Page

NETWORK ARCHITECTURE FOR NETWORK CENTRIC WARFARE OPERATIONS

1 SCOPE

This report is a delivery from the NBF-Grid project at FFI (Forsvarets Forskningsinstitutt).

The scope of this report is to roughly describe the mechanisms and functions required in a network architecture suited for the network centric warfare (NCW) concept. The focus is on the network services required to offer a robust, scalable and flexible network topology and architecture. The report does not describe applications, services and data definitions. However, it identifies the network components required to support both existing and future applications and services. Security architecture and services are not a part of the report and they will be analysed in a separate analysis.

Currently, all the NCW requirements cannot be fully met with the available technology and substantial further research is required. We have tried to identify the maturity of the areas. In particular we try to highlight the areas where military requirements substantially diverge from commercial requirements and where COTS (Common Off The Shelf) products are not sufficient, but specialized military solutions must be developed.

2 RECOMMENDATIONS

Each chapter contains detailed recommendations for a sub area. Therefore this chapter only summarizes the most important findings in bullet point format. The NCW has an architecture that must evolve as the technological abilities and the operational requirements change. With the current state of the art, the NCW goals cannot be fully met.

The most important recommendation is that all future applications and those under development should be made “future proof”. They therefore need to have an application programming interface (API) for setting important dynamic requirements towards the expected network services. The most important requirements that will have to be signalled are priority, QoS requirements, and multicast requirements. The following APIs need to be developed and implemented:

- API towards users and network administrators for setting priority and QoS requirements.
- API towards the network for expressing QoS requirements. The API should include both Diffserv and Intserv support. For application aimed at the tactical environment both modes must be available, since the QoS architecture in the tactical domain is open and likely to include both architectures.
- API for management of point to multipoint distribution of sensor and battle management data

In addition, all future applications should be IP dialect neutral, i.e. they should support both IPv4 and IPv6.

The expected NCW network topology is hierarchical and is likely to consist of three levels:

- A strategic backbone network, which provides access to national services and locations
- A deployable tactical network, which may be divided into two parts, a tactical backbone and tactical local/regional area networks. The deployable tactical network ensures connectivity between users that are unable to communicate directly due to different transmission technologies.
- A mobile ad hoc type network serving highly mobile units and users.

- Interdomain routing will be used between the higher levels in the architecture. BGP is so far the only alternative for interdomain routing (routing between the different nations and between the different NCW networks levels). The following areas must be addressed
    - Multihoming – most networks will have more than one external connection, for example the tactical network will both connect to other nations' networks and to the Norwegian strategical network. How to efficiently route traffic over the different interfaces will be a challenge and is not well supported by the current BGP protocol
    - BGP over satellite
    - Auto-configuration
        - BGP requires manual configuration, auto-configuration mechanisms should be developed to prevent misconfiguration.
        - It is difficult to debug the BGP protocol because of extensive use of local policies, mechanisms are required to ensure that faults are identified and fixed.
    - Load balancing is required to support not only routing based on shortest path.
    - BGP is not well suited for interconnection of mobile ad hoc networks since it relies on stable TCP connections.
- Mobility requires a combination of different mechanisms targeted towards specific types of mobility. No single mechanism will suffice.
    - At the tactical level, ad hoc and standard routing protocols should be used to support mobility.
    - Routing protocol and NEtwork MObility (NEMO) mechanisms can be used to support mobility of larger unit
        - NEMO is vulnerable for network partitioning
    - Mobile IP may be used to support limited mobility within fixed networks
        - Mobile IP is vulnerable for network partitioning
        - Mobile IP is well suited to support personnel mobility between nations
    - Role mobility will require support through the use of directories.

    - Mechanisms must be developed for efficient support of user mobility within tactical networks
- Multicast mechanisms must be implemented to support real-time information distribution to user groups
    - Routers/network switches must support multicast mechanisms
    - Security solutions must allow multicast distribution
    - Recommend that new distribution applications, typically sensors, support multicast and discovery mechanisms to identify information sources.
    - Real-time information distribution requires interaction between the QoS and multicast mechanisms; this is currently a research area.
    - Ad hoc networking and multicast is an area for further research
- CDN (Content Delivery Networks) are needed to support robust and flexible information publishing and subscription of non-real time data
    - Recommend the development of a strategy for the use of information proxies
- To support pre-emption for voice and selected data services as well as ensure a scalable QoS scheme, a combination on of IntServ and DiffServ is recommended. The RSVP signalling protocol is used for user-to-network and network-to-network QoS signalling.
    - New applications should support both a DiffServ and IntServ/RSVP API, this implies an API towards the users and towards the network
    - Mobile ad hoc networks will require specialized mechanisms
- Introduction of IPv6 is not recommended in the short term, but a procurement strategy is needed.
    - All new applications should be IPv6 enabled to ease migration.
    - All new networking equipment should be IPv6 enabled
    - Transition mechanisms are required to ensure interoperability with other nations deploying IPv6 prior to the Norwegian Defence.

3 INTRODUCTION

3.1 Architecture framework

The NCW network will be an Internet type network. However there are differences in the forces/actors forming the Internet and those forming the NCW network. These will be identified to better judge the possible development path.

Obviously, a NCW network should be an evolving network to take advantage of new technological developments. An important issue in the definition of the architecture is therefore to try to identify those issues that must be fixed initially and those that can evolve or be determined at a later stage.

3.2 Element in an architecture

Quote from "*Developing a Next-Generation Internet Architecture*" Robert Braden, David Clark, Scott Shenker, and John Wroclawski

" Network architecture is a set of high-level design principles that guides the technical design of the network, especially the engineering of its protocols and algorithms. To flesh out this simple definition, we have examples of the constituents of the architecture and how it is applied. A network architecture must typically specify:

- *Where and how state is maintained and how it is removed.*
- *What entities are named*
- *How naming, addressing, and routing functions inter-relate and how they are performed.*
- *How communication functions are modularized, e.g., into "layers" to form a "protocol stack".*
- *How network resources are divided between flows and how end-systems react to this division, i.e., fairness and congestion control.*
- *Where security boundaries are drawn and how they are enforced.*
- *How management boundaries are drawn and selectively pierced.*
- *How differing QoS is requested and achieved.*

Ideally, one would like to imagine using the architecture to "generate" the technical design, but making such a mapping in a mechanical fashion is clearly impossible. The architecture can only provide a set of abstract principles against which we can check each decision about the technical design. The role of the architecture is to ensure that the resulting technical design will be consistent and coherent – the pieces will fit together smoothly – and that the design will satisfy the requirements on network function associated with the architecture."

The NCW network architecture will only need to specify a subset of these elements. It is already given that it will be an IP based network. The protocol stacks to choose from are therefore in principle specified. The focus of this report is to describe the functions particularly required to support military operations and military applications and services. In addition the report outlines an operational network architecture suitable of supporting military operations nationally and internationally. This includes a description of possible internal interfaces and interfaces required for interconnection to coalition networks and public networks.

Two clear boundaries can be drawn, between the terminal/user and the network, and between the network elements within the network. The former is mainly an issue of the service that will be offered to the terminals or users. The later is a function of management requirements, operational procedures, administration and ability to scale.

Internet is today a mixture of client server and peer-to-peer architecture. Many terminals are not addressable directly, but function as clients connecting to servers. The NCW architecture is almost by definition a peer-to-peer architecture, where almost all terminals should be addressable. They must be able to act as both information sources and sinks. The information distribution will include terminals retrieving and sending information both in one-to-one and

one-to-many fashion. The network will therefore have to support push and pull distribution, both unicast and multicast.

The report does not define the security functions, management and operational functions and procedures required. Also an exhaustive list of services and application requirements are not presented, but the goal of the network architecture is to ensure an open and extensible network architecture capable of supporting most types of services, e.g. real-time services, multicast services, reliable and unreliable services, etc. The exact performance parameters supported by the network does not only depend on the network architecture, but also on the network topology, traffic characteristics and network element performance and can therefore not be calculated without a closer study of a detailed network design.

3.3 Development differences between NCW and the Internet architecture

The NCW should to some extent mirror the general Internet architecture. However, it will be shaped by forces or actors that are different from those shaping the Internet. Internet has in the last 10 years been changed to reflect the requirements of being a marketplace where the actors have different and often opposite goals. A premier example is the ongoing battle between music providers and those owning the IPR (International Property Rights) for the content. It has created new file sharing system and also created proposals for mandatory applications approved by the record industry. The NCW network will serve organization where the purpose of the actors is unified and charging is not an issue.

The security issues are also different. The threats and consequences of security breakdown are different. Similarly, authentication can be solved differently, since all legitimate users are under the same administrative domain (either nationally or internationally).

A fundamental force in shaping the Internet has been the requirement to scale over millions of terminals and ten thousands of alternative paths. As an example, the scaling forced the separation of naming space, administrative domain, and routing domains. Internet routing is based on aggregation of routes to minimize routing tables and routing table changes. The aggregation of routes implies restrictions on address allocation and mobility handling. The NCW architecture in a Norwegian setting will have substantial less need to scale. Backbone routers have routing tables with between 40 and 50 thousand entries, so it is not given that route aggregation must be used in a Norwegian NCW network. This is not an argument for abandoning route aggregation, but having a small network offers additional freedom in terms of the function that should be used for scaling reasons.

The timescales also have different granularities. In the Internet, provisioning represented in traffic engineering is of the order of time of day and lower. However, parts of the NCW network will have to respond to changes of the order of minutes or less. The appropriate mechanisms will therefore differ.

The NCW network will deploy transmission technologies that are similar to those found in Internet, but the technologies might be used at different levels. For example, microwave links are currently used in the backbone in FDN, while typically they are found in the access or metro level in the Internet. However, a NCW network must expect to utilize unidirectional

links to a substantial larger degree than in the Internet. This will have an impact in unicast and multicast routing protocols, transport and signalling protocols.

3.4 Military networking requirements

Current operational practice reflects the available technology, application capabilities and military operational requirements. In a NCW network all of these may change. The latter is an external issue to our investigation. The former two are to some extent migration issues. However, operational requirements based on existing technology may also generate general requirements that need to be questioned. As an example, the TADKOM voice service is based on reactive call routing. This enables user location and mobility handling and has the lowest blocking probability of all possible call routing schemes. However the cost is increased overhead, possibly a lower carrying capacity in the network (a function of topology, traffic matrix and link layer technology), and no robustness for ongoing calls against link failure. Although reactive call routing is the right choice for TDM voice systems, it may not be the optimal alternative in a converged NCW network where the routing scheme must be optimized for a combination of voice and data services..

3.4.1 Initial Internet requirements

The Internet architecture was developed based on a set of requirements [39]. The most important were:

- Inter-working: Existing networks must be interconnected
- Robustness: Internet communication must continue despite loss of networks or routers.
- Heterogeneity: The Internet architecture must accommodate a variety of networks
- Distributed management: The Internet architecture must permit distributed management of its resources
- Cost: The Internet architecture must be cost effective.
- Ease of attachment: The Internet architecture must permit host attachment with a low level of effort.
- Accountability: The resources used must be accountable.

3.4.2 NCW requirements

A NCW network will have additional requirements since it is expected to function in a highly dynamic environment. A NCW network must support:

- Mobility in terms of networks, terminals and users.
- Highly time variable resources: This is a direct consequence of the mobility. As the attachment point varies, the available resources are also likely to change. The dynamics in resource availability is also a direct implication of the dynamic usage pattern of sensor information that is to be expected in a NCW network where the sensor information can be substantial measured against the available bandwidth on the links.

- Allocation of capacity: With fluctuating resources and dynamic priorities an absolute requirement will be ability to allocate capacity. In next generation Internet, the allocation of capacity will have to be tightly coupled with pricing, accounting and charging. However, in a NCW network none of these issues are importance, since the network is under one management sphere with a clear understanding of priorities.
- Policy driven auto-configuration: The NCW will function in a dynamic environment where the availability of experienced administrators varies. The configuration of routers, servers, and end system should therefore be as automatic as possible. Since the environment and usage is expected to be dynamic, the configuration and operation of the network should therefore be governed by policies.
- Dynamic authorization: The authorization to use available resources will dynamically change, the time scale could be of the order of seconds.
- Ad hoc networking: Temporary wireless networks that organize and configure themselves will be needed. This could be viewed as a subset of the auto-configuration requirement. However, since it also has implications for the routing, it is identified as a separate requirement.
- Flexibility: The network will have to adapt to different operational practice, protocols and methods. International operations, with different partners, may be a common scenario.
- Timing constraints and synchronization: The existing networks are in many extents organized vertically, a separate network for each application. These applications may have synchronization and delay requirements that are integrated into the network technology. In an IP network, the network itself does not offer synchronization services. Instead this will have to be added as separate protocols or services like NTP (Network Time Protocol), or time stamping like in RTP (Real Time Protocol). Another dimension is that the existing applications are designed explicitly for the available network technology. The delay and jitter requirements may to a large extent reflect the constraints given by the current underlying technology. It may therefore be difficult to correctly identify the delay and jitter requirements. However, it is given that the synchronization needs should be addressed by several different mechanisms to reflect different scale and granularity requirements.

3.5 Incorporation of future technology

A network architecture forms the basis for the network design and guidelines for the introduction of new functionality and services. The network will evolve as new requirement or new enabling technologies emerge. The rest of the report will focus on the maturity of the different networking areas, and open issues. However, it is clear that the NCW concept will strongly benefit from emerging programmable and active networks technology.

3.5.1 Active and programmable networks

Current network operates under the paradigm of predetermined services. One possible development path is towards meta-services, i.e. the network contains functionality for the users/terminals to define their own services. Two such research paths are active networks and programmable networks. In the former, each packet contains its own processing instructions, while programmable network incorporates a signalling phase where the instructions for a flow are loaded into the network. The major research issues are the combination of defining powerful meta-services, while ensuring robust and predictive network behaviour.

Active and programmable networks are research issues and they are not technologies that can be introduced into operational networks in the next 5 years. A natural progression is policy services, programmable networks and then active networks, if at all. Including policy servers opens up for dynamic changes in network behaviour within given bounds. Programmable networks will offer wider functionality at a wider dynamic scale. Active networks will then extend this functionality even further.

3.6 Focus

In an architecture discussion, it is important to distinguish between functions that must be implemented in the end systems and those that require implementation in the network. In a NCW network end-to-end functions can relatively simple be changed and augmented, since all terminals are under the same administrative control. End system functionality can be added heterogeneously, i.e. only among those terminals that needs the functionality. As a minimum, an initial set of functions should be identified. Additional functionality can be added incrementally as the requirements emerge. However, the important issue is to clearly identify the functions that require interaction with the network. These cannot be added incrementally. Instead, they must be added to all network elements.

Originally, the end system to network interaction was minimal, restricted to naming and addressing. However, end systems with requirements involving predictable service, streaming or pushing of information, and network information retrieval, relies on state in the network. Network-to-end system signalling is there unavoidable. The focus of the architecture should therefore be on issues that involve network-to-network signalling and network-to-end system signalling, since these are the most costly functions to install or implement after the network is designed. Function involving Quality of Service, mobility, push/pull, and security should therefore be primary topics for the discussion. Security is analyzed in a separate project and it will therefore not be discussed here. All the other issues are discussed. In addition, interface to other networks, and immediate technologies like voice over IP and IPv6 are included.

An important part of the analysis is to identify open issues, with particular focus on issues where a solution is unlikely to evolve without an active research. Open issues or open problems can be classified into three groups, those that involve combination of existing standards, those where there is an ongoing standardization, and those that are target for ongoing research. IPsec and multicast is an example of the first group. Both are well define standards where the interface between them is discussed. However, the interface is not

extensive enough to cover combine deployment, and some additional standardization or proprietary development is needed. For the two first groups it is fairly certain that a possible solution will be developed. The focus of the analysis is therefore of identifying issues that are still in the research domain and are likely to remain there for some time.

3.7 Fundamental problems

The NCW network is an IP network. Although IP is a flexible technology there are some limitations. One limitation is the mismatch between signalling interface and security boundaries. A fully functioning IP network needs signalling between the end systems (terminals or leaf gateways) and the network. A security boundary across this signalling interface either limits the signalling, requires proxy signalling functions at the boundary, or multilevel end systems. It is outside the scope to discuss the strength and weakness of the various alternatives, since these to a large extent is a function of the operational and security requirements.

IP was designed to have minimal requirements towards link layer technologies, to be robust, and to allow for multiplexing. Originally, the ability to provide preferential packet treatment was limited. The QoS capabilities were therefore limited. However, the ensuing development of preferential packet treatment mechanisms in packet scheduling and buffering enables a wide range of QoS capabilities. The router implementations have also been optimised for preferential treatment. QoS is therefore not any longer a fundamental limitation. It is more an issue for suitable mechanisms, overhead and ability to scale.

A fundamental design choice for IP was the per packet forwarding based on source and destination address. Even though the routing protocols open up for different routing for different QoS classes, the common case is the lowest sum of metric or shortest path routing for all classes. The IP architecture does not have an aggregation level that would simplify different routing for different classes of traffic. Sharing the load onto different routes may be advantages from a resource utilization viewpoint. Although in sparse networks and wireless environment the advantage of different paths is limited or negative.

In principle, routing protocols can be developed that calculates different routes for different types of traffic. Augmented with dynamic installation of egress filtering to force traffic onto the calculated path, any type of path placement is feasible. However, the mechanisms would be proprietary and not be an integrated part of the architecture. The complexity would be needlessly too high. The alternative is to use an additional aggregation level, like MPLS and utilize the traffic engineering tools developed for this environment.

3.7.1 E2N signalling across an E2E security architecture

In a NCW network end-to-end functions can relatively simple be changed and augmented, since all terminals are under the same administrative control. End system’s functionality can be added heterogeneously, i.e. only among those terminals that needs the functionality. As a minimum, an initial set of functions should be identified. Additional functionality can be added incrementally as the requirements emerge. However, the important issue is to clearly identify

the functions that require interaction with the network. These cannot be added incrementally. Instead, they must be added to all network elements.

Originally, the end system to network interaction was minimal, restricted to naming and addressing. However, end systems with requirements involving predictable service, streaming or pushing of information, and network information retrieval, relies on state in the network. Network-to-end system signalling is there unavoidable. Functions involving security and mobility will typically rely on network state, and they should therefore be discussed in the network the end system interface.

4 TECHNOLOGY AND NETWORK ARCHITECTURE

4.1 Limitations

The Norwegian defence is being restructured towards a limited force that will be incorporated into a large structure. The arena is worldwide. The communication between the deployed force and the strategic backbone is therefore restricted to either satellite, tunnels through other nation's military networks, civilian VPN services, or leased line services.

The operations themselves are expected to develop towards a higher degree of mobility, where there may not be a clearly defined battle line. This implies a move towards aerial relay technology away from land based radio relay networks. A task force may no longer have control over the required relay points, and communication from a task force back to the command chain may instead be bounced through an aerial relay point.

This can be a combination of satellite access, low altitude and airborne communication platforms (UAVs), line-of-sight (LOS) and beyond line-of-sight (BLOS) solutions. The use of UAVs and satellites are likely to become more important since these are more flexible and can easily support mobile operations and rapid network topology changes.

The US military are planning to develop a large satellite base to support future operations anywhere in the world. This is not within the economic scope of the Norwegian Defence. Instead we must rely on a combination of using other nation's military satellites in combination with commercial satellites. As part of peacekeeping or coalition operations where it is important to quickly establish a military presence anywhere in the world, access to satellite capacity must be ensured. Depending on the market space of commercial satellite capacity, it may be necessary to engage in long-term agreements with commercial operators to meet the deployment constraints.

The NCW requirement on real time dynamic communication patterns also imposes restrictions on the deployed networking technologies and the topology. A hop over a geo-stationary satellite adds 250 ms delay. A radio link may add 10 ms delay due to interleaving, while the router's processing overhead may be in the 100 micro second ranges. The number of routers in itself is therefore not a significant factor, while the delay due to the load may be a substantial factor. It is therefore not sufficient to ensure connectivity between all possible force elements;

the architecture must also ensure some limitations on the number of hops. There are three principal choices to achieve this.

- They can use the same radio and link layer technology. Obviously, air, sea and land elements have quite different operating environment, and a common radio and link layer would be non-optimal.
- All routers in operational units have interfaces to all possible technologies. It is clearly infeasible to have different physical interfaces. Instead software configurable radio must be used. The JTRS (Joint Tactical Radio System) is an example of this alternative.
- The deployed units can have limited hierarchy with a common tactical backbone.

4.2 Network organization

For scaling reasons, the Internet is separated into interdomain and intradomain communication. The domains are named Administrative domains (Autonomous Systems), which are the unit for address allocation and interdomain connectivity routing using exterior routing protocols like BGP and MBGP (Border Gateway Protocol and MultiProtocol Border Gateway Protocol). The domains are further separated into routing domains, which can further be subdivided into areas. The domains play different roles. There are roughly seven backbone domains providing international connectivity. These are serving level 1 and 2 domains that offer connectivity at national or regional level. The lowest level is represented by AS offering access to customers. Clearly, there is not a strict one to one mapping between actor and domain, an actor may control and use several AS. The main advantage of the hierarchal approach is to limit the propagation of change or state. Between the different elements in the hierarchal structure, there are clearly defined interfaces for information exchange.

The NCW network building blocks mimic this organization. There are extended WAS (Wide Area Systems), LAS (Local Area Systems) and MS (Mobile Systems). However, it is not given that each element should be a separate administrative domain. The domain has a clearly defined interface, but the protocols are heavy in terms of operator knowledge, bandwidth, and overhead. However, if elements that within the same AS are reconfigured in new topologies or transferred to other AS, the management and configuration work can be substantial. We therefore recommend trying to avoid using the organizational interfaces if possible. From a NCW network topology viewpoint, there are three main types of networks, mobile (ad hoc) tactical networks, deployable tactical networks and strategic backbone networks.

5 NCW TOPOLOGY

We focus on the network requirements and capabilities necessary to support Network Centric Warfare. In addition, an enterprise network is required to support the daily administrative work of the defence. This is not addressed by the report.

5.1 Framework

We recommend a classical structure with three levels, a backbone, an aggregation level and mobile tactical networks. The aggregation network will play different roles depending on the operational role; it will either be a deployed tactical network or a tactical backbone network. The deployable tactical network is geared towards more static warfare and peacekeeping operations.

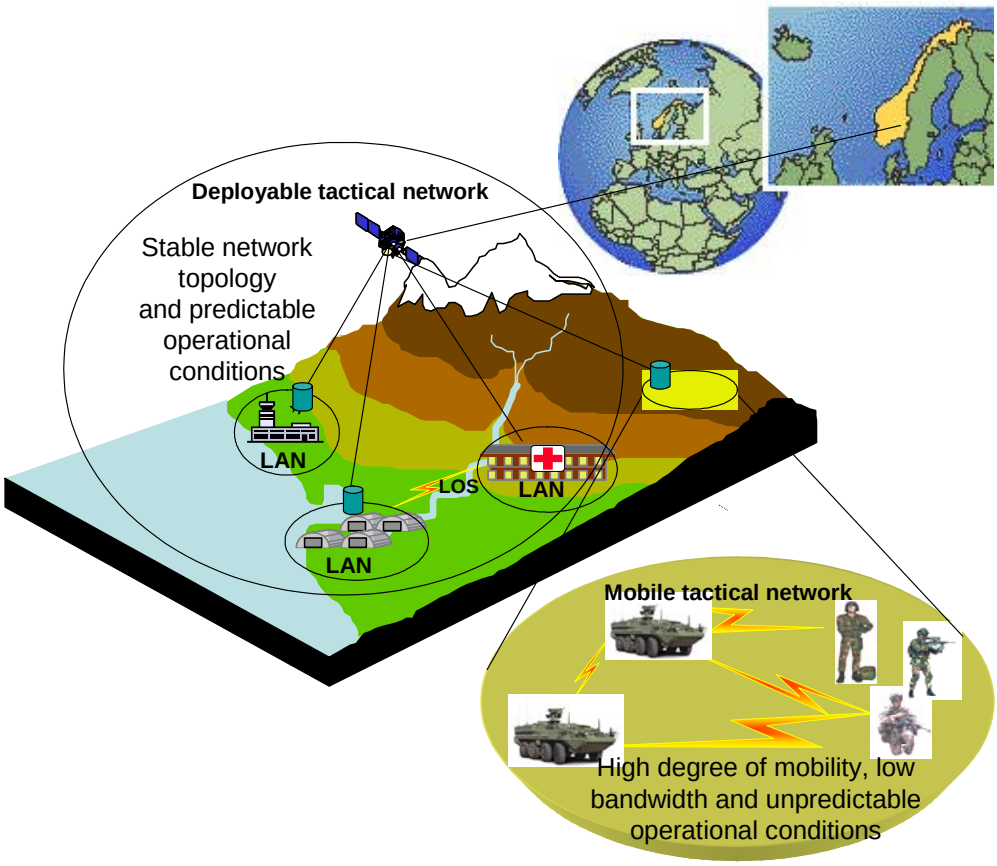

Figure 5-1: A three-level network topology

The two first levels of networks may be mapped to typical COTS network architectures. The strategic network can be viewed as an enterprise network consisting of a backbone, interconnecting access networks and local area networks. The deployable tactical network can be compared to remote branch office networks consisting of local area networks, which sometimes are connected to a local aggregation network and with a long haul access connection to the main enterprise network (strategic backbone network). The main difference when comparing a deployable tactical network to traditional branch office networks is that they may change their point of attachment to the rest of the network. Satellite and tunnelling will be the typical interconnection technology between the deployed tactical network and the backbone. In the former case, any geographic movement will be transparent. Otherwise the routing protocol of the backbone handles the change.

The mobile tactical network does not as easily map to a COTS network architecture and this also reflects the case that this is where military specific requirements have to be developed. Mobile tactical networks are flat wireless networks where all nodes are expected to be able to

forward traffic. The topology changes are signalled internally in the network, but there are no changes signalled outside the network. The topology of the network is expected to change since the nodes are mobile.

5.2 The strategic backbone network

The strategic backbone network will, for the Norwegian military, be a national network used to interconnect head quarters, access networks for sensors, bases, and tactical and operational networks. In addition it will also serve as a backbone for any international operations providing access to network services and applications.

Some nations extend their strategic backbone outside their national sovereignty, like the US which is in the process of establishing a worldwide backbone network based on IP, the Global Information Grid (GIG). This is not likely to be the case for Norway, as we have no fixed installations abroad. The Norwegian strategic network is therefore purely a national network.

5.2.1 The Norwegian strategic backbone

The main purpose of the strategic backbone network is to interconnect the access network for all national resources like sensors, HQ and bases, and the deployed forces. It is also needed as the interconnection point to other nation's strategic and tactical network. In addition, the national backbone network must be available for coalition forces operating in Norway both during peacetime and as part of military operations. Therefore, the national backbone network must offer standardised interfaces for interconnection to commercial networks and interconnection of coalition forces and national deployable and mobile tactical networks.

The network will be designed for stable operating conditions. The main requirements for the national backbone network are high capacity, robustness, sufficient geographical coverage, and operation and standardised interconnection points. The security requirements are analysed in a separate project.

The strategic backbone network will host a set of common services, which will be accessible from and replicated to the tactical networks. This includes authentication and authorization systems (Radius/Diameter servers), naming and directory servers like DNS, mobility registers (Mobile IP Home Agents), SIP/H.323 user information directories. In addition information servers (e.g. web servers) will host important information collected by national, coalition and international surveillance and intelligence sources. To offer interconnection to other networks, the strategic backbone should support, VPN and BGP peering points in addition to future possible standards like TACOMS Post 2000. Currently, the TACOMs Post 2000 project is defining a set of proposed draft standards defining the interoperability interface between national networks. It is discussed in more detail in section 9. The US DoD is also defining their information infrastructure and this work may result in requirements towards coalition forces networks. The VPN and BGP peering enables interconnection to commercial operators when switched services are used as access technology to international operations where Norwegian forces participate in. BGP is also a part of the proposed TACOMS standards.

The strategic backbone network will be based on IP and the network utilizes a variety of transmission and networking technologies. These will include everything from layer one technologies like leased lines to advanced VPNs over IP (IPsec and HAIPE), Frame relay and ATM. As the network will be the main interconnection point for all military operations abroad, interconnection to commercial networking services will be important. This will include everything from satellite accesses, telephony networks (ISDN and PSTN), and IP based services produced over the Internet or over dedicated IP based networks with high quality and availability.

Robustness is in this case mainly a function of the number of redundant paths (i.e. the degree of mesh) in the network and therefore a cost issue. The standard ways of increasing robustness is to increase the number of communication paths and to ensure that the communication paths are secured by physically being established over geographically different physical links. Typically a combination of different bearer technologies (fibre, radio and satellite) is used. However, switched services from different operators are attractive candidates for establishing a robust backbone network. The commercial IP, ATM, and MPLS networks have a substantially improved robustness compared to a few years ago. Use of public network operators will require service level agreements (SLAs) to regulate delivery conditions and define network and service availability and service quality. We therefore recommend that switched public services should be evaluated as an alternative, for example the use IP VPN services as these are more robust than leased line services. Physical robustness is likely to become less important as the threats to military networks are likely to move from physical attacks to cyber attacks, initiated both inside and outside the Norwegian borders.

Management of the national backbone will include management of the transmission technologies where these are operated by the military, network elements (routers, multiplexers), network services (DNS, Radius, Mobile IP, etc.) and application services (SIP/H.323, content distribution services, etc.). The network and service robustness will therefore also very much depend on the robustness of the network services and the management infrastructure and operational procedures.

Currently, the Norwegian backbone network consists of a transport network consisting of combinations of SDH and PDH radio links and fibre. On top of this there are three parallel service networks, which offer telephony services/delay sensitive data services, X.25 data services and the IP based InterLAN, which supports the administrative office systems, email and Internet access. A single strategic IP backbone is likely to have a lower network administration costs and improve bandwidth utilization. In addition, since an IP network may be overlaid many different transport and switching technologies, the number of possible suitable public network services will increase.

With the limited number of HQ, bases, sensors, access and tactical networks the backbone will interconnect, a standard routing architecture should be sufficient. A standard IGP (Interior Gateway Protocol) protocol, OSPF or IS-IS, have the required functionality and ability to scale. Possibly a two level hierarchy can be used. In section 5.3 it is recommended that the deployed tactical network should have the ability to use BGP for route exchange with the backbone. Obviously this capability will have to be reflected in the backbone also.

5.2.2 Other strategic backbones

The US GIG initiative includes establishing a global communication infrastructure utilizing both military and commercial network infrastructures. The wired infrastructure will be based on optical transmission.

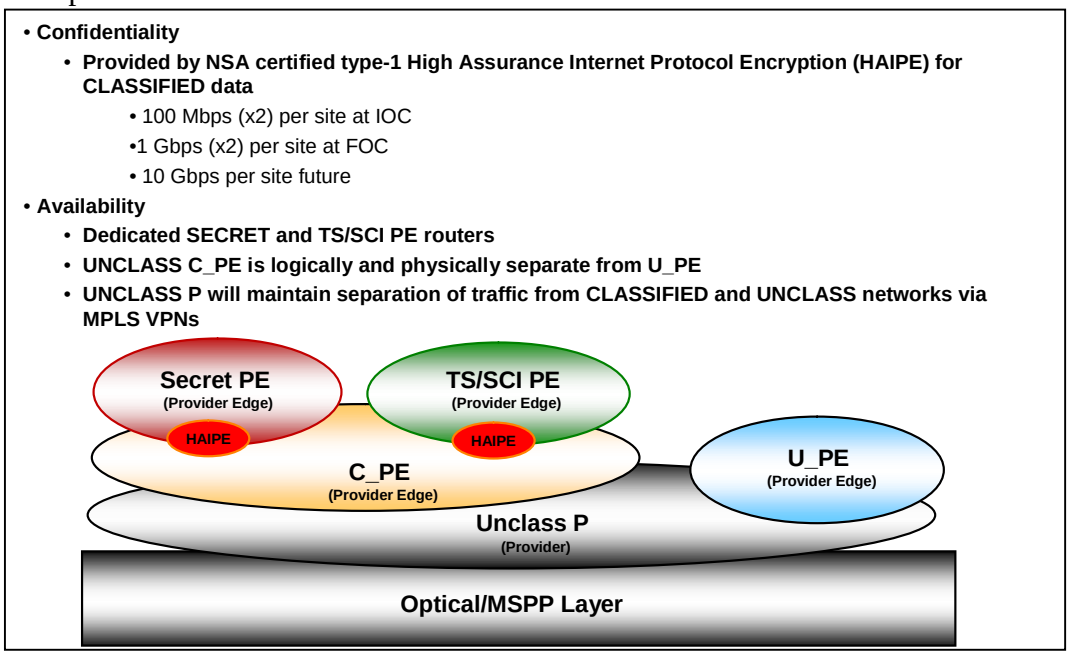

Figure 5-2: Planned IP Services Architecture (ref. Milcom 2003, Dave Mihelcic, Chief Executive Engineer for GIG-BE, DISA

Two classified and one unclassified IP based networks are overlaid an unclassified IP network and the classified and unclassified networks are separated through the establishment of MPLS VNPs. NSA High Assurance IP Encryption (HAIPE) is used to secure the classified network traffic. Legacy applications will until they are transitioned to IP be transported using a Multi Service Provisioning Platform (MSPP), which supports multiplexing of multiple networking technologies over optical networks.

5.2.3 Recommendations

To increase robustness, flexibility and limit the cost of network coverage and keep up with increasing bandwidth demands, it is recommended to deploy a larger degree of commercially available network services. By using a combination of transmission technologies, switched services and satellite links, and a more than one network operator the network vulnerability can be limited.

5.3 Deployable tactical network and tactical backbone

These are essentially the same type of network. The deployable tactical networks are operational networks that are established as part of international or national military and peacekeeping operations. The main requirements for the deployable tactical networks are to provide local connectivity at the operational site, possible aggregation of traffic and access back to the national strategic backbone network and its network and application services. The

deployed tactical network will also support a local operational infrastructure that will include local area networks for user access terminals and may include aggregation network if multiple local sites are supported. It is possible that 2G radio emergency networks like Tetra will be part of the network. These networks are defined for emergency operations and can therefore play a role at least in disaster relief operation. Tetra and similar types will be available as part of the infrastructure in some countries. Potentially, they could also be part of the deployed force communication equipment. Regardless, the deployed tactical network should have an interface to Tetra and similar type of network. The deployed tactical network can be compared to a remote branch network, typically established to connect daughter companies to the main enterprise network.

The tactical backbone is intended to serve mobile tactical forces, and it has most of the same functions as the deployed tactical network. It will supply the connection back to the strategic network. As important, it should be the common network for all types of forces. Any communication between elements in the same operating area should either be direct or through the tactical backbone. It should therefore have all necessary radio interfaces to communicate with any deployed forces, either directly or through a force specific aggregation network. The strategic backbone should consist of a subset of the equipment in the deployed tactical network.

Access to the strategic backbone network can be through the use of commercial operator's services or military communication networks. Possible access technologies are satellite, public ISDN/PSTN, public IP networks and/or military coalition networks. The use of public infrastructure may be limited in a war zone or in rural or less developed areas. Therefore, use of satellite will probably be the most important.

The Norwegian forces are intended to be elements in a large multinational force. As such it will be integrated into another communication's architecture. It is not given that naming and addressing will be the same or even compatible with the existing naming and addressing. It is therefore not given that the strategic and tactical network can be part of the same routing domain.

A deployed tactical network should support a wider set of services compared to those in the tactical backbone. As most operations last for months and sometimes years, both military and administrative applications and services must be made available. The most critical services and applications are best supported by establishing a distributed service architecture, where the main service node is located in the strategic backbone and distributed service nodes are established locally, e.g. telephony, email, messaging and services directly supporting the operation, e.g. situation awareness, local sensors, etc. Business services like logistics and personnel systems are less critical and may be located in the national strategic backbone network.

Remote network management and user support is critical to reduce operating costs and limit the number of expert personnel required to be part of the operation. Therefore, it is desirable to perform remote network and service management in a deployed tactical network. However, some management operations must be supported locally since they may need physical upgrades of the network devices and changes to the physical network topology. In addition, in

the role a tactical backbone, where the mobility is higher, management need to have the option of being performed locally; there is always the risk that the tactical network looses its connection the strategic backbone. Existing management applications do support central management, but the need to combine both central and distributed management is not as mature. Standards are not available, but products are on the market requiring the use of single vendor solutions.

5.3.1 TITAAN

The Dutch TITAAN network is an example of an operational tactical IP based network. It has been deployed in Afghanistan and interconnects the German and Dutch sites in the Kabul area and provides access back to Germany.

The TITAAN network consists of local area networks locally interconnected using radio links and with satellite access to the national strategic network. The network mainly utilizes commercial enterprise solutions based on IP for both data and voice applications. The solution is augmented with a QoS admission control mechanism to ensure the service quality of the voice traffic.

Experiences from TITAAN stressed the need for more advanced remote management solutions to provide a more cost-effective local operation limiting the number of local service personnel. Also the problems of using COTS equipment in very harsh conditions with lots of dust and where the maximum temperature may reach over 50 degrees Celsius and the minimum temperatures are well below freezing. As the equipment was not ruggedized, additional measures had to be taken provide additional cooling and cleaning. This resulted in a solution where all network nodes where duplicated to allow them to be regularly taken out of operation and cleaned and dusted. By taking these precautions, it was possible to provide a very stable network service, but it highlights the need for robust equipments capable of being used under different conditions. If this is not supported, extra manpower and duplication of network nodes is the only alternative under such conditions.

5.4 Mobile tactical networks

The mobile tactical networks will be deployed as part of national or international military operations. The mobile tactical networks are characterised by highly mobile units, users, vehicles, ships and aircrafts. Transmission between the units in the field is mainly based on radios and the communication nodes including the user terminals are all capable of acting both as end-user terminals and network relay nodes (routers). As the communicating units are constantly on the move, the network topology is very dynamic and requires special ad hoc routing protocols developed to support highly mobile nodes. The main limitations of the mobile tactical networks are limited bandwidth and the degree of topology changes which makes it difficult to predict the quality and availability of the communications services. The degree of mobility results in the need for special quality of service solutions capable of adapting to the changes in topology, communication bandwidth and traffic requirements.

Mobile tactical networks do not easily map into a typical COTS network architecture, since the technical characteristics of the mobile tactical networks are very different to the characteristics of available commercial mobile networks. The main differences are due to the high need for mobility and the use of network nodes both operating as end-user terminal and relay nodes. They cannot depend on the availability of a fixed infrastructure, for example base stations, which form the basis for commercial mobile networks. COTS-solutions for mobile tactical networks are therefore not readily available even though the standardisation bodies like IETF are developing IP-based solutions targeting the military requirements.

Depending on the type of communication technology used for the access to the backend network, the mobile units may have to change its attachment point to the backbone network as it moves. For example as a unit moves out of the UAV coverage, a satellite connection may take over as its primary access to the backend network. This will require solutions not only supporting user mobility, but also network mobility as the terminals operate both as end user equipment and network relay nodes. The changes can either be handled by the routing protocol or by specialized protocols like NEMO [1], which is an adaptation of the Mobile IP protocol. The solution to choose depends on the addressing scheme used for ad hoc networks. Currently, little effort has been spent on optimizing the interconnection of the ad hoc protocols to provide efficient and seamless routing between mobile networks and less mobile networks, e.g. tactical mobile network and deployable tactical networks.

Another challenge for mobile networks is to support network management and operational support. As the complexity and diversity of the services and network equipment increases, network and service management is becoming more complex. As it is not feasible to train every soldier to have complete knowledge of all aspects of network fault handling, fault management must be backed up by a combination of automated fault recovery procedures and centrally located experts. This is a challenging exercise and is beyond the current state-of-the-art technologies.

5.5 Routing organization

When all elements are under national command the networks can have a common routing domain. The number of routers needed to ensure communication with the available planes, naval elements and the mechanized brigade should be within a reasonable design envelope. The organization and communication needs of the National Force (Heimevernet) represent the uncertainties. The actual design cannot be made before the detailed communication structure for all forces have been determined.

The number of links between the tactical units and the backbone will normally be a few satellite and HF links. The backbone and the tactical network could therefore be organized as two routing domains with route filtering/importing or a formal BGP exchange across the link between tactical and strategic backbone. Internal changes in the strategic network connectivity will not reported to the tactical network consuming bandwidth over relatively narrow links.

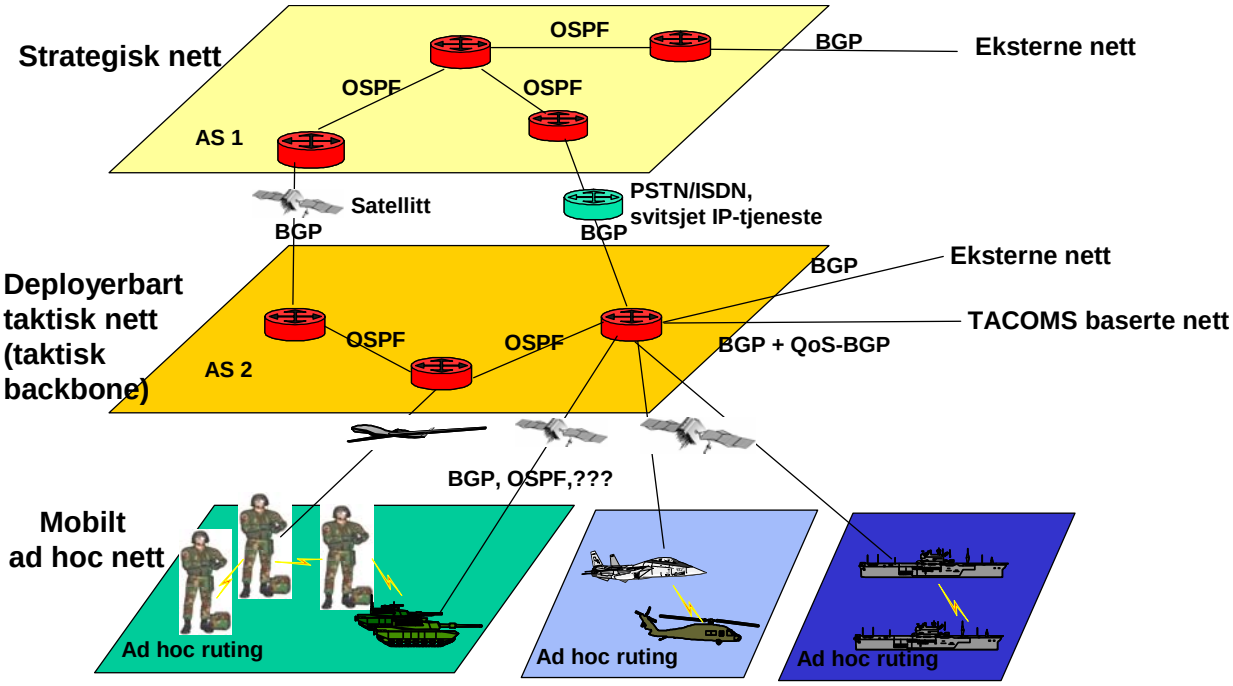

Figure 5-3: Routing between network hierarchies

The tactical elements will sometimes operate under multinational control. Normally there will be a communication link between the strategic backbone and the command structure of the multinational force. We postulate that additional communication links directly to the tactical force will be required. Possible motivations are: to ensure a direct national control over the elements, to ensure minimal delay or sufficient capacity, direct communication to logistic element, or to enable communication for personnel comfort. However such links represents a potential short cut in the routing. As long as all interfaces out of the network use BGP, the Norwegian network is a standard multi-homed network. There will have to be some coordination between the various BGP points to ensure correct traffic flow; for example traffic to the international HQ should not flow through the tactical network as long as there is another connection available.

If on the other hand, the tactical elements are integrated into the multinational force's own routing and addressing domain, the direct link represents a short cut of the routing. The solution is then either to use BGP over the direct links, or isolate the direct links by treating the national tactical elements as a private address space. Using BGP would be the architectural correct solution, since the direct link is just another link to a foreign address space. The disadvantage is that some of these may be narrow HF links. Isolating the direct links into a private address space with filtering NAT (Network Address Translation) servers between the rest of the address space and the direct links avoids the overhead of BGP. In order to be able to communicate with an element in the tactical force, there has to be mapping between addresses in national address space and addresses in multinational force. The mapping must exist in both the strategic backbone and in the tactical network. Only for a limited set of terminals can such a mapping be allowed and maintained.

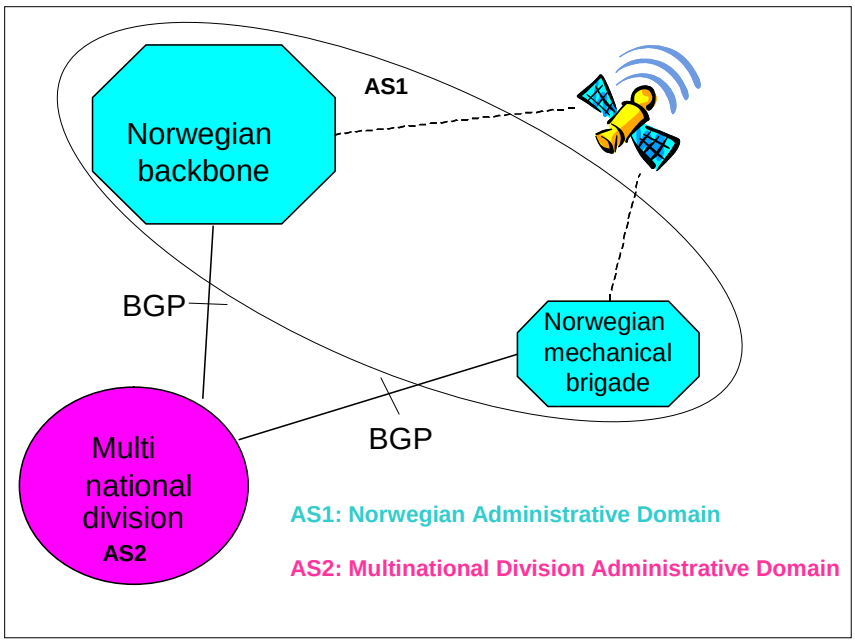

Figure 5-4: Illustrates the communication paths when a mechanized brigade is allocated to a multinational division as a separate national element. The interface between the different elements will be BGP or have BGP as important element.

The determining factor for the routing architecture will be the routing and addressing structure of the multinational force. However, using BGP at the deployed tactical network or the tactical backbone is always a possible solution. We therefore recommend that BGP capability is part of the deployed tactical or tactical backbone network.

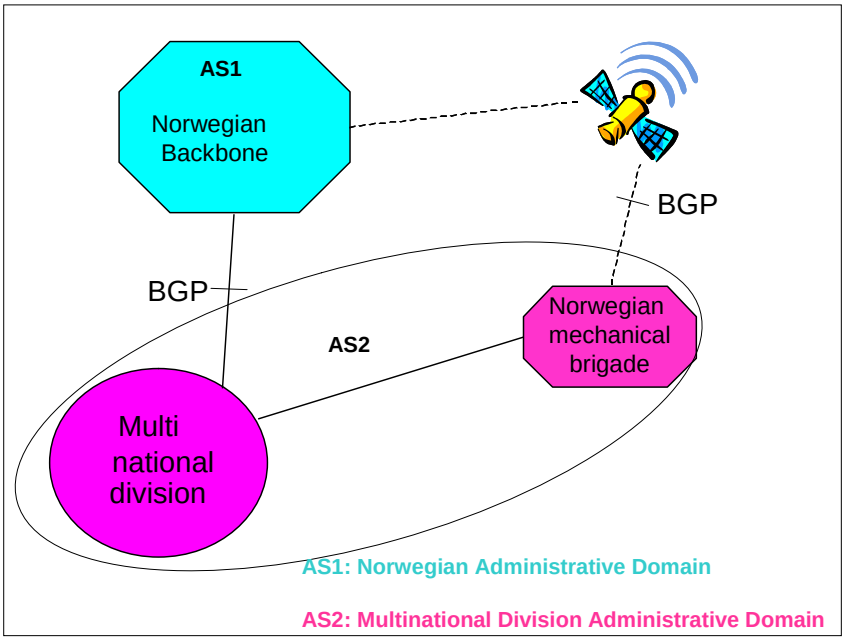

Figure 5-5: Illustrates the communication paths when a mechanized brigade is integrated into a multinational division. The interface between the different elements will be BGP.

6 MOBILITY

Mobility is a fundamental part of the NCW concept. The goal is to analyze whether any mobility technologies can be excluded, and as part of that process identify the usability of the various technologies. The default hypothesis is that the different mobility requirements of NCW can only be satisfied by a combination of different technologies.

6.1 Types of mobility

There are any different types of mobility a system potentially must cope with. A fundamental difference is whether the mobility is transparent or not. With transparent mobility, ongoing sessions are supported during the mobility. Another important distinction is the communication scenario, whether it is dominated by client-server or peer-to-peer traffic patterns. In a client- server paradigm, the client communicates with a limited set of well-known servers. The servers respond to requests from the clients, and they have a limited need to track the location or identity of the clients. Most of the needed information can be signalled with the request. In a peer- to- peer scenario, the terminals potentially must be able to communicate with any other terminal. Also, they are also as likely to initiate a communication flow as they are to respond to a request. In order to initiate a conversation, the clients/terminals have a need for location information to locate the other clients/terminals in the system. A NCW network will tend towards the peer- to- peer communication model, imposing stricter requirements of maintaining location information about the other terminals/users in the system.

6.1.1 Role mobility

At the highest level, there is role mobility, where the role or function may move around to different users, or groups. Examples of a role are company commander, postmaster, or S3. An important aspect of role mobility is the context of the role. If role mobility is to be transparent, it also requires context transfer in a broad sense. This is an application design issue, since “required context” depends on the role. However, it may imply support from the network itself. For example, if full hot stand role mobility is to be supported, the network may have to support reliable multicast transfer

6.1.2 User mobility

This category covers situations where users log on to different machines/terminals. The machines have fixed IP addresses and the association between user and IP address changes as the user logs on to different machines. Such a scenario is suitable for client/server communication, but difficult in a peer-to-peer scenario. Users must then register themselves at a directory each time they have changed to a new machine. The typical example of user mobility is an Internet café where users log on to web based services.

6.1.3 Distributed processing

In distributed processing, functions or data can be shipped to different servers. It involves mobility, but normally the mobility is realized as a separate overlay network or as part of middleware independent of the functions in the network. Mobile code and agents can also be classified under this heading. Distributed processing should be considered as part of the middleware functionality.

6.1.4 Terminal portability

Terminal portability covers the situation where a terminal is moved to a different location. The terminal is assigned a new IP address and additional context information like default routers, SIP gateways and DNS servers. The move need not be to a different physical location. Terminals can be placed in different logical networks while remaining in the same location. Examples of terminal portability are lap tops connected to an ISP either through ADSL or GPRS. With portability, all sessions are terminated before the terminal is moved. Terminal portability in a peer- to- peer scenario will, as with user mobility, require the user to register with a directory server each time the terminal's address is changed.

6.1.5 Terminal mobility

Terminal mobility is a derivative of terminal portability, but under mobility ongoing sessions are maintained when the terminal is moved. This requires that all flow identifiers are maintained, and a two tiered IP addressing model is used. The first tier uses the terminal location as an address, and it is changed as the terminal is moved. The second tier represents the flow id and remains constant during the lifetime of a flow.

6.1.6 Chain of mapping in IP

Classically, Internet has four levels of indirection, name, IP address, path and MAC address. A name maps into a destination interface IP address. The address maps into a path to the destination and a MAC address in the end point (physical interface). The difference between the path and MAC layer address mapping represents the difference between layer two and layer three routing or switching. By indirection, we mean logical stages where one entity is mapped into another. All of these indirection points can be used for handling mobility. The indirection is also recursive, a name can be mapped to another name, or an IP address mapped to another IP address.

Originally, there was only a mapping between fully qualified name and an IP address. The mapping was done by the domain name system, a global hierarchal naming tree with limited service. However, this functionality has been extended to mapping of service to name, capability to terminal and authorization to user. Although, the functions of DNS are still an important part of Internet, directory systems with broader capabilities are often used. Examples of such are SIP and network operating system types of directories typically built on top of LDAP [37].

IP addresses are allocated statically through management, or dynamically through DHCP [33], zero configuration protocols [18], proprietary mechanisms, or IPv6 address discovery mechanisms [36]. These mechanisms may be supported by additional authentication and authorization protocols like radius and Diameter [35].

The mapping of a destination interface IP address to a path is done by the routing protocol, either one suited for a wireline environment or one more adapted towards mobile wireless systems or ad hoc protocols. The destination is mapped to the address of the next hop towards the destination with standard IP forwarding. However, the mapping of destination address to a path or route need not be direct. Instead there can be several recursive steps, like two tiered addressing or IPsec, where a destination is mapped to tunnel endpoint, which is again mapped to a path.

The next hop in the path must be mapped to the underlying link technology. Again, the mapping can be recursive, where the path is mapped to a layer two tunnel like MPLS. The mapping mechanism is located in the router where a next or last hop address is mapped to an interface, a tunnel or a MAC address. If the next hop is mapped to a tunnel, each type of tunnel has its own signalling mechanisms. If the next hop is mapped to a link layer address, the dominant mechanism for destination address to MAC address is the ARP (Address Resolution Protocol).

6.2 DNS

DNS [34] is a specialized directory aimed at primarily translating between a logical name and IP address. Additional capabilities include mapping of services to logical name. It is one of the fundamental parts of Internet and it has evolved for more than 20 years. It has a fairly complicated structure. However from a mobility discussion it is sufficient to understand 1) the inherent limitation in terms of frequency and time between mapping updates, and 2) the robustness.

The naming structure is a global tree with domain as the elements in each level. The bottom level is the name of the individual terminal. The unique name of a terminal is the concatenation of all domain names along the path from the top to bottom in a dot-separated notation. The first level has 5 international domains (edu, com, org, mil, net) plus all national domains. Each domain can delegate authority for parts of their name space to others. Names will therefore have variable number of levels. When part of a namespace is delegated (called a zone), there needs to be a pointer to the server responsible the new sub domain. To resolve unknown names, the fall back strategy is to start with the rightmost domain and identify the server that can resolve the next component of the name. The procedure is applied recursively until the name is resolved or proven non-existing. The underlying assumption is that all nodes directly or indirectly know the servers responsible for the first level (the rightmost part) of a name.

This will clearly not scale. For example, every access of a web page generates one mapping request. The top-level server would therefore be swamped. The basis for DNS is therefore a substantial use of caching. Mapping of domains to servers and mapping of logical names to addresses are cached each time they are requested. Servers can generate answers based on

previous cached data. Only in exceptional cases will a mapping request be sent to the top-level name servers. All mapping elements have a time to live field (TTL), stating the maximum time they can be cached. Items can only be removed from a cache by aging out, and there is no invalidation since the owner of a mapping has no knowledge of where the mapping is cached.

If DNS is used for mobility management, the TTL field sets the boundary for the maximum time it will take until a move is registered. Only when a mapping is aged out of all possible caches can other corresponding nodes reliably detect a move. The cost of a short TTL is an increase in the load on name servers, since short TTL values result in low hit ratio on the caches.

Originally, DNS was only a global naming tree. However, as long as the nodes in a system know where to start a resolving process, the naming tree can be local. This is a technique that has evolved in response to the development of intranet. Within a corporation, the naming structure can have a substantial finer granularity than the one that is viewable externally. (Only a few names should be resolvable from the outside for example www and e-mail servers, while all PC should be resolvable from the inside.)

Initially, the mapping for a domain was stored in a flat file and a change of name or address was handled manually by editing the file. All servers should have backup, and the consistency between the copies is based on polling and sequence numbers.

For mobility management is this not sufficient and the mechanisms must be extended. There are two main directions; one is a dynamic updating mechanism within DNS and one direction aimed at the changing the underlying storage structure for the naming content of a domain.

Dynamic DNS is a proposed standard that allows updating of a domain’s naming records. It requires stable storage and support for atomic transactions. The updating need not be authenticated, but a proposed standard specifies a shared secret and public/private key scheme for authentication. Authorization and updating policies are local issues. A clear disadvantage is the lack of updating transactions covering several domains. An automated scheme for mobility management will encompass erasing mapping in old zone and creating the updating in the new zone. This should be done as an atomic transaction, either by the DHCP servers or by the terminal itself. Regardless, it is not a standardized, and will have to be implemented as a proprietary scheme supported by the combination of DHCP/DNS server or DNS server and terminal. In addition, it can only be implemented within the same administrative domain, since the policies for authentication and authorization of update request must be the same for all involved mappings.

6.2.1 Directory used as repository for a zone

The alternatively to having a dynamic updating scheme at the DNS level, is to use a directory to store the mapping information in a zone. The updating and replication mechanisms in the directory can then be used to update the mapping in DNS. The difference is only in the mechanisms used for updating the information, the restrictions and implications on the updating remains the same. The advantage is in the simplification of procedures, the same mechanism is used for all updating of information; there is not a separate mechanism for IP address mapping and another mechanism for other type of information.

6.2.2 Analysis of DNS

DNS is not usable as a global general mobility handling system for rapid terminal portability or mobility. However within a limited scope within one administrative domain, it is a feasible mechanism. The limited scope is given by the need for short TTL values, which increases the load on the servers. Alternatively, no caching is used with a proprietary replication mechanism to the servers. Regardless, the scope must be limited, since the updating /replication mechanisms only scale within a limited scope. The one administrative domain is a restriction implied by the updating mechanisms. If they are to operate automatically, the updating policies (i.e. security and authorization) must be identical. In addition, there are no standardized transaction mechanisms for updating between different domains, implying the use of proprietary solution within the same administrative domain.

Role mobility, i.e. the role of a user or terminal is changed, is most suitable supported by the DNS. For role mobility one is essentially mapping a logical name to a terminal. The alternatives are either to change the mapping between role and IP address of the terminal whenever the role is changed, or to keep the mapping between role and IP address fixed and instead change IP address of the terminal. The latter is inadvisable. It means an outside event will trigger a reconfiguration of the terminal, and therefore also most likely of the sub-network. It will terminate all ongoing sessions. The mechanism is vulnerable, since if the system has some inconsistency in role assignment, the same IP address will be assigned to multiple terminals, which will force a shutdown of the terminals in question. In addition, no such mechanism is standardized, and it is likely a difficult procedure to make automatic regardless of network architecture and topology. It is therefore recommended that role mobility is handled at the DNS/directory level.

6.3 Directory

Directories are data repositories aimed at application with multiple readers, with a need for dynamic queries, with a high ratio between reading and updating queries, and with a weak consistency requirement. Within these confinements, it is possible to avoid the high overhead of the strong consistency in a distributed database. In mobility management, directories can be used in different setting, for example for mapping between role and name, phone directories, location directories for VoIP, service locations and service description, repository for configuration data, and as a storage component for DNS.

Directories use partitioning and replication to achieve robustness and minimize access delay. In partitioning, the information is divided among several servers, while replication ensures multiple copies are available at several servers. The two strategies can be combined with parts of the catalogue replicated to a subset of the servers.

Replication represents a trade off between robustness and overhead. The availability increases with the number of copies. In addition, the response time should be shorter, since there is a higher probability of finding a repository close to the client. The disadvantage is an increase in the overhead due to maintaining consistency between the different copies.

Replicated directories must solve two main problems 1) how to ensure consistency among the various copies and how to locate the servers where data is being stored.

6.3.1 Consistency

A directory needs only to ensure that eventually all replicas will be consistent. The mechanisms to distribute updates and to ensure consistency between updates need not be as strict as in distributed databases. Directories schemes can be grouped depending on whether updates must be done through a master node or whether all or a subgroup can perform updating (multi-master). The latter alternative is more robust, but the cost of a more complex consistency mechanisms. In a NCW setting, multi-master is almost always the sole alternative, unless the directory only has a terminal/vehicle local scope.

In directories, there is a risk for inconsistency in the data if updates are lost, or multiple users update the same data almost simultaneously. To resolve inconsistency, the operations or the data values must be ordered sequentially, either by time stamping or through a numbering system. As the updates are being distributed from replica to replica, the inconsistencies are resolved. Within a reasonable time synchronicity, regardless of the order of updates, a consistent view of the correct value can be reached. However, it may require that deleted data is kept to enable a rollback

The replication topology typically is configured manually. This is the state of the art for the dominating IETF standard (LDAP [37]), which is supported by most major manufactures. The topology can either be direct, where an update propagates directly to all other servers or partial with store and forward mechanism where updates are propagated to a subset of the servers directly. The updating can either be of push or pull, i.e. in the former a server with a new update propagates the changes to all its partners. With a pull based updating, the servers will periodically poll each other for changes. The optimal choice is a trade off between overhead and the time it takes to reach consistency.

6.3.2 Server location

The server location problem is divided into how to find the information tree and how to navigate in an information tree. Normally, the navigational information is part of the tree. The tree itself will contain information of the servers storing information at a higher and lower level in the tree. How to find the tree itself is normally handled by a combination of well-known addresses, service location protocols, and configuration. It is a well research problem, and the problem is mainly one of matching mechanisms to traffic pattern and topology.

6.3.3 Analysis of directories

Directories, as a repository/retrieval system, will continue to be a part of future network systems. Concept like Directory Enable Networking (DEN) from DMTF (Distributed Management Task Force, www.dmtf.org), which is supported by several major manufactures, is an example of this trend. However, the impact directories will have cannot be evaluated solely based on technical features. As important is the information that is stored in it and how the information is used by an organization. The active directory from Microsoft is an example.

It is multi- master LDAP directory with some proprietary extensions. As such, it is a general-purpose directory. However, it is also integrated into the authentication and authorization of users. Among the registries is a repository with user summary information to more easily allow users to log onto any terminal within an organization. The rule of thumb is that a new replica requires approximately 40% of the whole directory to be copied. This does not reflect the overhead of a LDAP multi-master replication, but how the information is structured and how the various terminals and users use it.

To summarize, directories will be an important part of future systems. However there is a balance between robustness, overhead, access delay and consistency. In addition, the type information stored and how it is used by a system affect the balance. The issue is therefore not whether directories should be used, but the role they should play in mobility management. Potential usage areas are repository for authentication/authorization, configuration information, VoIP mapping from name to location or IP address, DNS zones, or location information in mobile IP.

Due to the inherent robustness requirement in NCW network, the various mobility management schemes must have distributed update and storage structure. Directories can play two different roles. The mobility management scheme can be a centralized one implemented on top of a replicated directory, or the scheme can be distributed where the directory only has a local scope with a limited robustness. Clearly there can be combination, for example a hierarchal system where directories are used differently at the various levels. In a centralized scheme, the overhead and the robustness are increasing functions of the number of servers. The convergence time is also an increasing function of the number of servers. A centralized scheme on top of distributed directory will therefore have a limited ability to scale. Directories are therefore more likely to play a role as data repositories in distributed mobility management solutions. There is not a well-defined boundary on the usability of directories. Instead it should the case-by-case trade-off between operational requirements for robustness, information content, usage patterns, and capabilities of the underlying network.

6.4 Address assignment

Terminal portability is a default function found in almost every network. Terminals normally get their addresses and required contexts from DHCP servers. As long as the terminal is able to authenticate itself towards the DHCP server, it will be assigned an address. The weakness is the updating of the mapping between name and address. This was discussed in section 6.2. The DHCP server need not be a single point of failure. Two alternative solutions can be combined. Additional DHCP servers can be kept in hot standby, or multiple servers can serve the same terminals. In the latter case, the servers offers addresses and context information and the terminal selects the server with the most appropriate offer. There is no standardized mechanism for coordination between servers, so the servers must be assigned disjoint address rooms.

In an IPv6 system, the address assignment is simpler, since a terminal can construct its own address based on broadcast information from the nearest router. The mechanism is

supplemented with a broadcast message from the node to verify that the selected address is unique.

The mechanisms for terminal portability are well understood. The weakness in a peer-to-peer setting is the dynamic updating of the naming information. It is therefore a mechanism suited for terminal portability within one administrative domain. The dynamic configuration is aimed at terminals and they are not suitable for routers. Although, the mechanisms are well understood, they are still being improved within various working groups in IETF.

6.5 Routing

In principle, mobility can be handled as a special case of links breaking and new links coming up. The routing protocol can therefore in principle handle mobility. However, it is only feasible in limited scope.

The routing protocols consume memory space in the routers to store the routes, processing power in the routers to calculate the routes, and bandwidth to distribute the status of links or routes in the system. In order for routing to work on a global scale, the routers are organized in a hierarchal order with addresses assigned so routing entries are likely to aggregate in the hierarchal ordering. The hierarchal ordering ensures that updates have a limited scope. The aggregating address assignment ensures fewer routing entries and therefore also fewer updates.

For the routing to scale, addresses must be assigned to aggregate and there must be a limited updating traffic. Routing as a general mechanism to handle mobility is therefore inconceivable; each move would imply periodic updating messages from the moving node that would have to be distributed to the whole network. However, within one administrative domain or a routing domain it can be used; the moves will not be distributed outside the domain, and the effect of route aggregation is limited. Routing is particularly adapted to handle network mobility, where whole sub-networks change their attachment points. The exact scale of which routing can be used to handle mobility is a function of the frequency of the mobility, whether it is single terminal or network mobility, the type of routers available, the number of routers, the link bandwidth, and the required switchover time.

6.6 Two tiered addressing

The two tiered addressing is a principle aimed at proving session transparency. A mobile host uses two addresses, one to designate its logical network attachment, and one as an identifier for connections. A packet destined for a mobile node is routed using the attachment address to a FA (Foreign Agent) where the packet is forwarded to its destination. The original address is translated to the attachment address by an address translation function. The mapping between the addresses is in a location catalogue that needs to be updated by an updating protocol each time the attachment address is changed. The functions can be placed at different location, so several architectures can be realized with two tiered addressing. We will look closer at three alternatives that illustrate the span in the possible architectures. These are Mobile IPv4, Mobile IPv6 and a distributed scheme used at the Columbia University in the mid nineties.

6.6.1 Mobile IPv4

The address translation function is placed at a home agent (HA) located in the home network of the mobile node. The HA must be able to intercept all packets destined towards nodes that potentially can be mobile. It is therefore often located at the router interfacing the Internet. The underlying assumption is that the network is single homed, i.e. only one router connection to the network. The intercept mechanism is not standardized, but proxy-ARP is an often-used mechanism. At the attachment point the forwarding is either done by a specialized device called a foreign agent (FA) or by the mobile node itself (co located forwarding). In the former case, the FA is responsible for allocating attachment addresses, while in the co-located case other mechanisms like DHCP must be used. The two tiered addressing can be misused to hijack addresses and thereby intercept or fake all communication to the node. The HA, FA and the mobile node must therefore authenticate and authorize the various operations. In the Internet this represents a problem, since there might not be a common level of trust between the three elements. In a NCW network, this should not be an issue, since the elements are under the same administrative domain. Packets destined for a mobile node are always tunnelled from the HA. From the mobile node they can be sent directly to the destination as long as the forwarding only is done based on destination address. In an enterprise environment, egress filtering is often used as a safety precaution. The mobile node must then tunnel all flows back to the HA that will do the forwarding towards the destination.

Multicast can either be done using double tunnelling where IGMP (Internet Group Management Protocol [6]) messages are tunnelled back to the HA and the multicast streams are forwarded through the tunnel. The alternative is for the mobile node to use its attachment address in the initiation signalling (IGMP) and the stream is forwarded directly from the source. In the latte case, session transparency is not achievable.

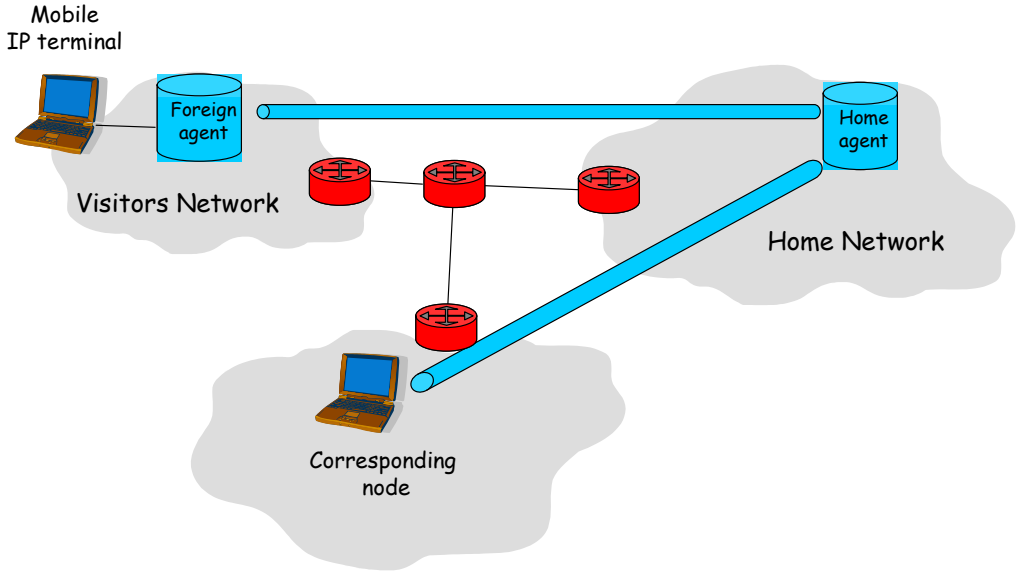

Figure 6-1: Mobile IPv4 architecture

6.6.1.1 Analysis

The HA represents a single point of failure in two different aspects, it maps from home address to attachment address, and it is one point where all flows must go through. The mapping itself can be made robust by standard load-sharing techniques. Several nodes can share the responsibility. Incoming packets are hashed to the set of available HA. Packets from the same source are then always mapped to the same HA as long as the HA is functioning. The registration from the mobile node the HA is periodic and therefore need not be robust. In the event of a failure it will eventually be correct. Alternatively, the result of the registration can be broadcasted to all HA, so the all have a complete picture of the context. They will be in hot standby and can take over the mapping on a per packet basis. To the mobile nodes, the HA can appear as one logical address. Well-known load sharing mechanisms at IP or link layer can be used to direct the messages to one particular HA. In addition, mobile IP also has its own mechanism for discovering different addresses that can function as a HA. The registration message can be directed to a multicast address. The registration will be denied, but the response message will come from a valid HA. The source address of the reject message can then be used for a new registration message. The address translation function and location register functions in the HA are therefore single points of failure that can be made robust by standard techniques.

However, Mobile IP assumes that all flows from a corresponding node will go through the HA. In a partitioned network, a corresponding node will be unable to communicate with any mobile nodes in their own partition that has HA in the other partition. The HA must be on the path from all potential corresponding nodes to the home address. If the home networks are physical networks, they therefore tend to be placed at leaf nodes, where the robustness is limited.

The home network may also be a virtual network, i.e. its only physical representation is the HA. It can then be placed in more robust sections of the network where it is less vulnerable than as a leaf node. The down side is limitation it will have organization. All potential mobile nodes must belong to the same network and only pre-selected terminal can be mobile. As long as there are only a limited number of mobile nodes, the virtual network is on option. However, the performance is a substantial more complicated scaling problem compared to placing the HA function distributed at each physical network. Regardless of organization of the HA, the solution is vulnerable to partitioning in the network.

6.6.1.2 Triangular routing

In Mobile IPv4 all packets to a mobile node is routed through the HA. In principle the mobile node can route packet to the corresponding node directly along the “optimal” path determined by the routing. The packets can use the mobile nodes original address as source. The packets in a bi-directional flow will therefore not take the same path and they will form a triangle. In most enterprise environment, firewalls and routers do egress filtering allowing only packets from its own domain to emerge from an enterprise. In these cases, packets from a mobile node will have to be tunnelled back to the HA. It is cannot be excluded that similar security policies can be used within the leaf networks in a NCW network.

6.6.1.3 Performance

The hand over process, when a terminal moves to a new foreign agent, is relatively slow; a new context must be established with the new foreign agent, the new temporary address must be communicated to the home agent. In addition, a tunnel back to the old foreign agent to handle all packets still in flight must be established. All of these signalling processes should be protected by authentication protocols.

Mobile IPv4 relies on tunnelling for all traffic to the mobile node. For voice traffic over low bandwidth links, there is not only the issue of header compression for the IP header in the tunnel packet, but the inner header with the original header needs to be compressed as well. The tunnelling also raises QoS issues.

6.6.2 Mobile IPv6

Mobile IPv6 utilizes the options in the header to avoid triangle routing and the use of an explicit FA. All mobile nodes are capable of allocating their own attachment address, and co-locating is the only option for forwarding. When a mobile node receives a packet from a new destination it registers its attachment address with the new source. The corresponding node maps from the identification address of the mobile node to the attachment address. The address translation is moved from the HA to the corresponding node itself. However, the HA is still needed for initiation of all flows originating outside the mobile node. The triangle routing is therefore avoided.

6.6.3 Columbia scheme

This is a mobility scheme aimed at a restricted environment. All mobile nodes are located in separate address ranges. There are dedicated routers handling the mobility. Each has control over the mobile nodes attached to it (over wireless links). The dedicated routers do the address translation. Packets aimed at a mobile node are routed to the dedicated router closest to the packet source. The router maps the address to the dedicated router responsible for the mobile node and forwards the packet to it. The router responsible for the mobile nodes handles the actual forwarding. The normal routing ensures that packet for a mobile node are sent to the nearest dedicated node that is capable of handling the forwarding. The location registry is located at all the dedicated routers. Lazy evaluation is used for updating. If no mapping exists, a request is broadcasted to all routers to find the one that has the mobile node attached. That mapping is used until the forwarding is no longer valid. The dedicated node receiving packets for forwarding to a node it no longer has attached will send an error message, and a new broadcast will have to be made.

This is an optimisation of the scheme used in TADKOM. The disadvantage is scaling abilities. The location request must be broadcasted. When nodes are moved, the updating of the new location is a slow process. The advantage is the robustness. To initiate or maintain a flow a corresponding node need only to find a router that has the location information. There is no single point of failure it is not a standardized scheme.

6.7 Ad hoc networking

In an ad hoc network there is no infrastructure except the terminals themselves. The network can be an independent island, or one of more of the nodes can be connected to a global network. Each terminal must be capable of forwarding traffic. Even though an ad hoc network can consist of a mixture of terminals and routers, it should be considered a mobile router network. An ad hoc network is characterized by:

- A dynamic topology where the links can change randomly and rapidly.
- Links with limited dynamically changing bandwidth. A radio link in itself will have changing characteristics. These are enhanced when both sender and transmitter are moving. In addition, the interference from other moving nodes will be variable. Compared to a wireline environment, the available bandwidth is limited. The overload of links will be a more common event that in a similar wireline network. In addition, in a radio environment, links need not be bi-directional.
- Potentially the nodes may have some constraints on the energy that can be used. In some usage scenarios, the battery capacity is limited. In addition, there may also be some constraints on the willingness to be exposed. The exposure is not only a function of the traffic a node creates, but also of the traffic it forwards. In ad hoc networks, the objectives of the routing protocols can therefore be different than those found in regular networks.
- The network is more vulnerable, since it is based on wireless technology. In addition, in order to cope with the dynamic topology, the antennas have fairly broad coverage; in many cases omni directional antennas are used.

The protocols designed for ad hoc network tend to blur the layered approach. With a limited bandwidth, the emphasis is on optimal utilization of the available bits. A standard routing protocol is inefficient for typical ad hoc scenarios. In an wireline environment, one aspect is aggregation of addresses, while in an ad hoc environment, the addresses cannot be aggregated; two sequential addresses are seldom in the same geographical or logical neighbourhood due to the dynamic in the network.

Instead specific routing protocols have been developed. These are optimised for different usage scenarios and topologies. It is unlikely that there exists “the optimal” protocol. Instead, different protocols for different scenarios are the norm. The routing protocols can be classified into four groups, flat with a reactive routing, flat with proactive routing, hierarchal, and geographic position [12].

With flat reactive routing, a node does not maintain any topology information. When a node has to send information to a new destination, the route to the destination must first be discovered. Typically a request is flooded through the network until it reaches the destination or a node that has a current route to the destination. The scheme is based on the same principle that is used in call routing in the TADKOM system. Typically, the protocols use mechanisms for identifying the bi-directional links, since the discovery mechanisms will not function across a uni-directional links. Reactive routing trades delay in the first packet against potentially

lower overhead since topology information is not maintained. The scheme is best suited for uneven traffic matrixes, with bursty communication with a few other partners.

The proactive flat routing represents an optimisation in the different direction. It maintains full or partial information of the topology. Link information is flooded through the network. The difference between the various protocols is in terms of the selection of the nodes that will do the flooding, the frequency of the flooding (can vary based on the number of hops), and whether all or only some links are reported. The protocol family is best suited for even traffic matrixes where the nodes communicate on fairly regular basis. The overhead of maintaining topology knowledge needs to be amortized over the flows that utilize the knowledge. Proactive protocols have a full and partial topology map and they are therefore more suited for uni-directional links.

Hierarchal protocols typically use different routing schemes. Nodes are clustered, and one routing scheme is used within the cluster, while between the cluster controllers a different scheme is used. Such schemes are favourable in particular when there is cohesion between the nodes, like soldiers in a squad or a platoon. Other hierarchal schemes use different routing schemes based on the traffic to a node. Nodes, which are popular destination, can “afford” to maintain topology information, while for nodes that are seldom part of a conversation a reactive routing scheme may be more suitable.

The last class of routing schemes are based on geographical position. The packets are routed towards the destination based on the coordinated of the destination and the coordinates of the neighbours [13]. In terms of overhead, these protocols are lean, since they need only to maintain topology knowledge of the one hop away nodes. Typically, packets are forwarded to the neighbour that is closest to the destination. However, it is not given that all nodes on a path is closer to the destination than the predecessor, a fail back procedure is needed. The disadvantage is the cost of maintaining the position of the possible destination. Several different methods, proactive, reactive and hierarchal have been proposed. The overhead of a geographical routing must also incorporate the cost of maintaining knowledge of the position. However, in military systems, this is in itself often a goal.

6.7.1 Analysis of ad hoc networking

The alternative to ad hoc networks is to always have a fixed infrastructure within the transmission range of al nodes, like in GSM or UMTS. As this is infeasible in typically military scenarios, ad hoc networking will be a part of a NCW network. It is a fairly accepted “truth” that no routing protocol will fit all possible ad hoc usage scenarios. The specific features of the ad hoc network require optimisations at the various protocols levels that are not optimal for wireline environments. The ad hoc network should therefore be treated as a separate type of network. However, one possible outcome is that a standard routing protocol, like OSPF, is adapted.

Ad hoc routing, in spite of being a research area for more than 30 years, is still in it infancy. The IETF has a working group focused on ad hoc networking, but it has still not produced standards. However, it has successfully been an arena for development of candidate protocols.

One important aspect of ad hoc networking is the tight integration between the various layers. The functionality at the physical and link layer need to reflect and be reflected in the networking and application protocols. This should not be interpreted as a desired towards the vertically integrated systems. However, it emphasizes the need for flexibility. Different usage scenarios will require different routing protocols that may have different requirement on the services at the lower layers.

Ad hoc networking is still therefore an area where research and development is still in high need. However, it is not only a routing protocol issues. Roughly speaking, the research in ad hoc networking can be subdivided into the following areas

6.7.1.1 Configuration

The underlying assumption for many of the protocol proposals is that the nodes have fixed IP addresses. From a strictly routing viewpoint, there is no need to have IP addresses. The addresses are not aggregated, and any unique address is sufficient. However, for inter-working with other network, it is an advantage that the multi-hop nature of ad hoc network is not hidden. IP addresses should therefore be used. (The LUNAR protocol is an example of the opposite [14]). It is feasible to extend the mechanisms for dynamic allocation of addresses to apply for ad hoc networks. However, in a peer-to-peer environment, there is a need to map these addresses to logical names. There are several ways to do so, ranging from dynamic updating of DNS to two tiered addressing, as discussed in previous sections. However, within the confinement of dynamically changing networks additional restrictions are imposed, and there is no general agreement on a preferred solution. It is therefore a topic for further research and development.

6.7.1.2 Routing

The focus in ad hoc networking has been on connectivity. Emerging issues are QoS, call admission and measuring resource utilization. There are also investigations into useful load sharing mechanisms. However, these issues are investigated in the setting ad hoc networks being single homed stub networks or independent networks. In a NCW network, we expect the ad hoc networks will have a more complex topology and in some cases may even function as relay networks. The open issues of routing, load sharing and resource allocation and call admission needs to be investigated also for these challenging environments.

6.7.1.3 Topology control

The topology is controlled by multiple factors, the movement of the nodes, the physical environment around the nodes, the radio effect, and by the directional control of the transmission. The physical environment and the movement of the nodes are external factors. However the development of electronically steered directional antennas and power control enables topology control. Topology control enables optimising the relationship between efficient routing and interference from other nodes. With fixed power, the optimal number of neighbour in a fixed environment is a little less than six. As movement is introduced, simulation experiments indicates, that the optimal is around 8 to 12. There are many proposals

on integration of directional transmissions and routing and power control and routing. Given the multitude of routing protocols for different usage scenarios, one would expect a similar research and development effort of integrating power and directional control. Topology control is therefore likely to remain a rapid developing research area.

6.7.1.4 Policy control

Within a wireline environment policy control is a hot topic. It is focusing on how to formulate and enforce different policies on how a network should be utilized. Particular focus is on QoS, load sharing, access control and call admission. In an ad hoc environment policy control should be even more important, since the restrictions are even more rigid. Overload situation will occur more frequently due to the dynamic topology coupled with the variable capacity. In addition, energy usage imposes additional challenges. There will have to be formulated polices on how limited battery reserves should be spent on forward traffic. As the network evolves, the routing protocols may have to change optimisation goals from shortest hop to maximizing remaining battery reserves. The nodes in the network may also operate under different rules. An example is silent nodes, that only receives but do not transmit. Such nodes can only participate for a limited time in an ad hoc network, before its position has aged out of the topology map. However, the combination of directional antennas, power control and optimised routing protocols can be utilized to minimize the exposure. A few bytes sent to the nearest neighbours at minimum power fairly infrequent may still provide enough information for the other nodes in the network to continue sending information. The semantics of such a policy formulation, i.e. the trade off between exposure of the silent nodes, and the overhead in the network is a research issue. It is more so an operational issues, since it enables new functionality at the cost of a higher risk.

6.7.1.5 Management

In ad hoc networks, the nodes move around. For faultfinding and fault isolation there will therefore lack a reference point. An additional challenge is that faultfinding and repairs reconfiguration will have to be done remotely. It is unlikely that the level of expertise available at the individual nodes (personal radio, vehicle, or tank) will be sufficient for more complex management operations. Management in ad hoc network therefore pose additional challenges that need to be investigated.

6.7.1.6 Security

Security is analysed in a separate investigation. However, we would like to point out that in an ad hoc environment the security challenges are even more formidable. In particular, since every node participates in the routing it is substantially simpler to modify and manipulate the routing information.

6.8 Mapping at link layer

In an environment with homogenous radio technology and a fixed infrastructure with access points or base stations, mobility can be handled at the link layer. The GSM/GPRS/UMTS systems are proof of the suitability for link layer mobility under this restricted scenario.

For ad hoc type of scenarios where there is no infrastructure, it is inadvisable to handle the mobility at the link layer. For the network layer it would hide the multi-hop nature of the network. At the network layer all nodes would appear as being on the same subnet. For broadcast and multicast traffic special solutions will have to be engineered in order to avoid wasting resources on blindly broadcast unneeded traffic to all nodes. Similarly, there would be interference with the QoS, resource assignment and routing at the network layer. The resulting resource usage is highly likely to be non optimal. This would interfere with the routing at the network layer.

6.9 Analysis of mobility schemes

Mobile IP has a limited usefulness. It is the only alternative if session transparency is required when a terminal moves from one link layer technology to another in an environment with a fixed infrastructure. If there is no infrastructure, ad hoc networking is the only alternative. If there is movement within the same radio technology, link layer mobility techniques or ad hoc networking are more appropriate. If the mobility is restricted to a limited scope, utilizing the routing is an option.

Mobile IP is vulnerable against network partitioning. It requires either an organization that places the home network of mobile nodes where the connectivity is robust or a research and development of a more dynamic placement of the HA similar to the scheme used at Columbia University.

The session transparency is unlikely to be a requirement. It requires a background radio service that is available whenever the node moved out of the coverage of the primary access point. This is the primary usage examples in the COTS world where GSM/GPRS/UMTS acting as a backup when a node moves out of a wireless LAN coverage zone. Most likely such technologies will be available only in limited cases. Regardless of whether such technologies will be available, it would imply that all potential mobile nodes must set up and maintaining a session over the back up radio technology whenever there is a risk that the node will move outside is primary attachment. In addition to using up radio resources, it would also mean unnecessary EMC exposure.

Mobile IP should be used as attachment technology when directory cannot be updated since the update will cross several administrative domains. In principle, such usage scenarios can be served by dynamic updating of DNS or directories. However, these are not protocols that are suited for usage across different administrative domains due to the need for common authentication and authorization schemes. In addition, the ability to scale is limited due to the need for short time to live on the cached information. A typical usage scenario would be a liaison officer attached to foreign unit. Mobile IP is used for all communication from the home

network to the officer. For all traffic to and from the foreign unit, role mapping based on DNS or directories could be used.

6.10 Recommendation on mobility

All technologies for handling mobility should be deployed. Ad hoc routing protocols will be the dominant mobility handling technology at the tactical level. In this area there are many issues that cannot be resolved without a substantial research effort. For units with a home address in the strategic network or one of the HQ, bases or sensor network, Mobile IP will be suitable. However, some standard robustness techniques for the Home agent may be required. For units that have a home address on a wireline segment in a tactical network we recommend development of additional mobile protocols. In the literature there are several examples of suitable robust protocols aimed at deployment within a limited scope.

7 QUALITY OF SERVICE IN NCW

QoS features at IP level give improved and more predictable network service by providing the following intelligent services:

- Support of dedicated bandwidth
- Loss and delay guarantees for the most critical applications
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network and ensuring that the most important traffic takes precedence during network overload.

In a military network, the QoS architecture additionally needs to be designed to handle the following:

- Graceful degradation in cases of severe network degradation
- A dynamic quality and priority differentiation targeting changing operational requirements

To handle prioritisation of users and applications, the QoS design for NCW networks cannot purely rely on packet prioritisation, but requires additional functionality to reduce the total amount of traffic entering the network avoiding massive congestion. If traffic entering the network is not controlled, packet-buffering mechanisms are not sufficient to shield the most important traffic from loss during severe congestion [44], [43]. Therefore applications or application proxies must be able to signal their resource requirements. The network elements must also be able to refuse the establishment of additional traffic flows and police the incoming traffic. This is in particular required in the part of the network with limited bandwidth or where frequent topology changes results in changes to the offered bandwidth. Use of IntServ with RSVP signalling offers a solution providing bandwidth, delay and loss guarantees for high priority flows under different networking conditions. Combined with the use of DiffServ classification and marking making it possible to only support DiffServ in parts

of the network or during topology changes where reservations have not been confirmed offers a scalable and flexible solution, see [45].

7.1 Scope

QoS refers to the ability of network elements (for example, applications, hosts, or routers) to support some level of assurance in order to ensure that the traffic and service requirements are met. QoS has end-to-end significance. Enabling QoS requires the co-operation of all network layers, as well as every network element from end-to-end. All parts of a protocol stack will affect the resulting quality of a communication session.

The degree of QoS achievable depends on the network topology, bandwidth and link quality, the inherent properties of the transmission system, its available QoS functions that intelligently can control the network's resource usage, and the performance and scalability of these QoS functions.

This chapter will focus on the IP QoS mechanisms and the capabilities and relative performance of these functions. The actual performance of the functions in terms of scalability and processing overhead also depends on the router design.

7.2 QoS requirements

The QoS requirements on bandwidth, delay, delay variations, packet loss and peak rate will depend on the applications needs and the requirements on prioritising critical user traffic. The main difference between the two types of requirements is static versus dynamic QoS. Applications QoS requirements are more or less static based upon some operational (e.g. the users expectations) and implementation decisions. For example the choice of video and voice codecs and some applications will loose synchronization if packets are lost due to high delay or delay variations. The requirement to prioritise critical user traffic is dynamic and depends on operational aspects. An ideal QoS architecture for the NCW network should have the following three main properties:

- Be able to maintain the QoS requirements in terms of bandwidth, delay, delay variations, packet loss and peak rate that the applications need to function properly during normal operation.
- Flexible division of network resources allocated for different levels of traffic importance, ensuring that the available network resources are allocated to the most important traffic. Ideally, the quality of service requirements should be ensured for the *admitted* traffic.

Since one of the greatest advantages, of packet switching systems like IP compared to traditional circuit switched networks like TADKOM, is the effective utilization of bandwidth. Therefore, the QoS architecture should provide good bandwidth utilization.

The requirements on graceful degradation will affect the QoS architecture, i.e. graceful degradation on per flow level has different requirements compared to graceful degradation on per class of service. In a normal situation, the best utilization of network resources is assured by a rather coarse handling of flows. As the network degrades, different QoS policies might be

required, enabling mechanisms supporting a stricter per flow degradation for types of traffic that can not function under sever packet loss and even a complete blockage of certain types of traffic not considered as important. The main problem with this scheme is that the notion of importance is very operation specific, and may change relatively frequently. This need for dynamic policy support is very different to commercial network operations.

7.3 QoS architectures

This chapter gives a short summary on the status of the current IP QoS mechanisms and technologies. A lot of effort has been used to standardize, define, and develop IP QoS systems, but a complete and mature architectural framework and operational techniques covering a diversity of network technologies and operational constraints are not yet in place.

DiffServ [19] has matured over the last few years. Building blocks like queuing, policing and traffic shaping are proven functions and commercial available routers support the DiffServ Per Hop Behaviours (PHB). Currently four standard PHBs are defined to construct DiffServ enabled networks and achieve coarse-grained end-to-end QoS. There are also management systems with some restricted functionality to manage and control the policy and monitoring in DiffServ networks.

IntServ [22] offers a per flow control through reservation of resources and support for priority pre-emption. IntServ has suffered from scalability problems (e.g. the handling of hundreds of thousands of short lived flows through a high capacity core networks is a problem). Although some of the scalability problems have been solved, IntServ is not widely deployed.

MPLS-TE has been developed to offer a scalable solution for managing and delivering QoS in backbone networks. MPLS-TE support aggregated DiffServ QoS for MPLS paths over broadband core networks. MPLS-TE is available in commercial routers, but the technology is still in a very early stage and flexible and dynamic traffic engineering management tools are not widely available.

7.3.1 DiffServ

Differentiated Services defines the architecture for implementing scalable service differentiation in the Internet. The DiffServ service model is easy to manage and satisfies differing QoS requirements at a relative coarse granularity (theoretically 64 different classes). This architecture achieves scalability by aggregating traffic classification state, which is conveyed by means of IP-layer packet marking using the DS-field. Packets are classified and marked, and receive a particular per-hop forwarding behaviour at nodes along their path.

Classification, marking, policing, and shaping operations need to be implemented at network boundaries or hosts.

7.3.1.1 Classification

Classification of packets is based on the application/protocol being transported, and a set of network parameters like source and destination address and port number.

Classification performed by the hosts allows for a more dynamic operation compared to the edge classification. Dynamic edge classification and marking depends on the presence of a signalling/management system enabling the user to signal their requirements to a policy manager, which then informs the network edge device. The advantage of the latter is that it allows for a level of control, not leaving the decision entirely to the user/application.

7.3.1.2 Packet marking

The packet marking/re-marking process writes the differentiated services code point (DSCP [25]) in the IP-header, which further gives the information on how to forward the packet inside the DS-domain. Packets that have entered a DS-domain and are marked with the same DSCP and crossing in a particular direction are forwarded in the same manner and are therefore told to be of the same Behaviour Aggregate (BA). To achieve end-to-end QoS for packets traversing several DS-domains, Service Level Agreements (SLAs) define how BAs are mapped between the different DS-domains.

7.3.1.3 DiffServ PHBs

A PHB refers to the packet scheduling, queuing, policing, or shaping behaviour of a node on any given packet belonging to a BA. There are currently defined three standard PHBs to construct DiffServ enabled networks and achieve the end-to-end priority and service quality. They are the best effort PHB (default), Assured Forwarding PHB and Expedited Forwarding PHB.

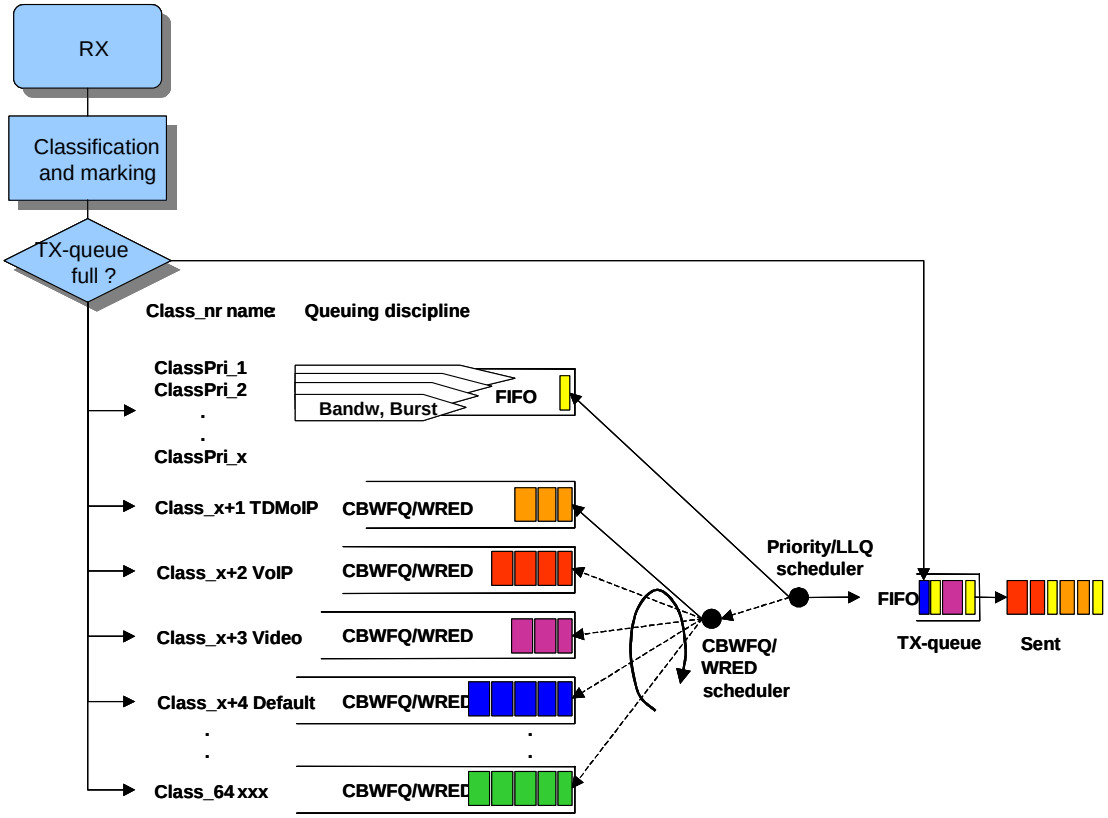

Figure 7-1: Example of DiffServ functional elements

7.3.1.4 Assured Forwarding PHB

The Assured Forwarding (AF) PHB is defined in [21]. AF PHB defines a method by which Behaviour Aggregates can be given different forwarding assurances. There are four classes AF1, AF2, AF3, and AF4. Each class is assigned a specific amount of buffer space and interface bandwidth. Within each AF class three drop precedence values can be specified. The requirement is that there is a higher probability that packets of the higher drop precedence will be dropped before packets of the lower drop precedence.

The drop precedence method penalizes traffic flows within a particular BA that exceed the assigned bandwidth (measured by a policer). A possible policing policy would be to remark out-of-profile packets.

In military networks, the drop precedence could be used to let the applications mark the importance of the traffic. Note that this is not the intended usage of the drop precedence as specified by the DiffServ architecture, but this use should be transparent to the core routers.

7.3.1.5 Expedited Forwarding (EF) PHB

The Expedite Forwarding PHB is defined in [20]. The EF PHB is used to providing a low-loss, low-latency, low-jitter, and assured bandwidth service. Applications such as voice, real-time video, and military real-time tracking and weapon systems require such a robust network-treatment. Although, EF PHB when implemented in a Diffserv network provides a premium service, it should be specifically targeted toward the most delay and jitter critical applications. If the network experiences congestion the EF class ensures that the delay of this traffic is not affected. It is not possible to treat a large amount of the overall traffic as delay critical or high priority. This would result in either high packet loss or longer delay, as the buffer lengths for the high priority and delay sensitive traffic must be increased. The problem of using EF as it is defined is today is that there is no drop precedence within the EF PHB giving all EF traffic the same drop probability.

7.3.1.6 Explicit Congestion Notification (ECN)

With ECN a router can mark packets that have experienced congestion. ECN could be useful to enable applications to support admission control. This assumes that applications can be trusted to take the appropriate action, once the packet destinations report the congestion. The experimental RFC 2481 [26] describes how the Currently Unused (CU) 2-bit field of the DS-byte can be used for explicit congestion notification (ECN) in DiffServ. Routers are generally not providing an ECN service.

7.3.1.7 Multi-Level Expedite Forwarding PHB (MLEF PHB)

Currently the EF class does not support multiple priority levels or drop probabilities, but there is a draft proposal defining an extension to the EF PHB allowing support the multi-level precedence and pre-emption. This is achieved by introducing active queue management and advanced drop mechanisms for the EF queue making it possible to treat packets with different priorities differently.

This scheme is similar to the solution presented in [43], where we show that it works well for low levels of congestion, but for high levels of congestion there is no way to prevent packet loss also for the high priority traffic. Also it lacks mechanisms for preventing additional traffic to enter the network and it also lacks mechanisms to signal to the user that the reduced quality of the call is due to congestion and that the call should be terminated. The same arguments are also presented in [44].

7.3.1.8 Challenges and possible solutions

DiffServ enables scalable and coarse-grained QoS throughout the network, but has some drawbacks, as it does not offer admission control. DiffServ has the potential to support multicast traffic, but the network dimensioning is complicated as multicast trees and memberships changes frequently.

DiffServ networks needs to be carefully provisioned according to the expected traffic characteristics (SLAs). Given the limited number of levels of drop precedence and the static provisioning of classes, an optimal provisioning is required to fulfil the QoS requirements for the admitted applications and at the same time completely gracefully handle network degradation could be difficult to achieve.

Network resources are allocated to traffic streams by service provisioning policies, which govern how traffic is marked and conditioned upon entry to a differentiated services-capable network, and how that traffic is forwarded within that network. However, the main problem is that even with the use of DiffServ both EF and AF, under-provisioned links should be protected from sever overload since massive overload will result in deteriorated service quality for all traffic. For the network to stabilize, the traffic must be policed and prevented to enter the congested part of the network. Ideally, policing should be performed by the first hop router and any place where data streams converge and may enter a congested link.

Policy based QoS management and Bandwidth Broker solutions have been defined as an approach to provide more flexible control of the use of the network resources during different operating conditions by controlling the network load. An example of this type of functionality is SIP proxies at ingress/egress points that limit the number of simultaneous voice sessions. This main problem with this scheme is that the SIP proxies have no knowledge of routing and relies on either a very conservative provisioning strategy or assumes only a single entry/exit point to the network.

Another mechanism offering control of the network resources is the use of IntServ. This however requires maintaining state in the network.

7.3.2 IntServ with RSVP

Using the IntServ QoS model, Resource Reservation Protocol (RSVP) signalling [23] can be used by applications or proxy agents to signal their QoS requirements to the network. Queuing mechanisms are used to provide the following IntServ defined services:

- Guaranteed Rate Service, which allows applications to make reservations with quantitative guarantees on delay, jitter, packet loss, peak rate etc at IP level.

- Controlled Load Service, which allows applications to have low delay and high throughput even during times of congestion. For example, adaptive real-time applications such as playback of a recorded conference can use this kind of service.

The IntServ model enables flow based admission control. The QoS policing management model might be used to specify and provision the admission control policy.

Flow based QoS is not considered scalable in large IP networks since state information for each individual flow must be kept in the router. With end-to-end flow based QoS signalling, reservations specified by quantitative QoS parameters can be guaranteed since the admission control will check on the available network resources. Flow based reservations (like IntServ with RSVP) will scale if a relative small part of the traffic needs this service or if reservation are aggregated in the parts of the network offering very high bandwidth..

A Policy Manager (PM) can be used to support admission control with pre-emption, in an IntServ environment.

The scalability argument may not hold if only some portion of the network resources are reserved for use with aggregated RSVP [42].

7.3.2.1 Challenges

The uncertainties about use of IntServ in military networks are:

- RSVP requires dynamic signalling by the applications or by proxies. RSVP is available in operating system APIs, but not commonly supported by applications.
- User to network signalling is currently not supported by the IP crypto solution although this is standardised, RSVP Extensions for IPSEC Data Flows" [41] and "RSVP Operation over IP Tunnels" [40].

Even though use of native RSVP for parts of the traffic will scale in a military, RSVP introduces signalling overhead, which may become relatively high in low bandwidth networks. Aggregation of RSVP flows may be used to limit the overhead, [42]. This allows routers, which handles a large amount of flows, to use the DiffServ code points for packet prioritisation. Aggregate RSVP is signalled by using the DCLASS object in the RSVP PATH message. This allows for the combination of DiffServ and IntServ type QoS handling in the network. For example can RSVP be used at the network edge controlling the traffic entering the network, and DiffServ may be used in the network core or when transporting traffic over IPsec tunnels which hide the individual traffic flows.

7.3.3 Traffic Engineering

MPLS Traffic Engineering (TE) [30] mechanisms are used to complement the QoS mechanisms. Traffic engineering (TE) is an important tool to ensure that IP traffic is load balanced across parallel links/paths in the network. This reduces network congestion and increases the ability to support the QoS requirements for time critical traffic and to give more efficient bandwidth utilization. TE can also support some degree of QoS based routing (e.g. analogue to a routing protocol with different metrics).

Commercial use of MPLS TE is mainly in backbone networks between routers. It operates on aggregated flows and applications are not assumed to be able to support the TE signalling. MPLS TE will be used in fixed backbones, but the use of MPLS TE in wireless networks is uncertain since the traffic engineering applications are not assumed to be dynamic enough to support rapid topology changes. Therefore MPLS is likely to be supported in the strategic networks.

Two approaches are defined depending on the degree of resource utilization required. In an environment where only a limited optimisation of network transmission resources is required, DiffServ and MPLS TE might be used to operate on aggregate basis across all DiffServ Behaviour Aggregates. In this case, DiffServ provides the per hop prioritisation, while MPLS TE offers a better distribution of the aggregate traffic load. This is called DiffServ MPLS.

If more close control of the network resources is required it might be possible to do traffic engineering on a per class level instead of on an aggregated level. This is referred to as DiffServ aware Traffic Engineering (DS-TE).

7.3.3.1 DiffServ-MPLS

Two approaches are used to support DiffServ MPLS [29]. They rely on the definition of two types of Label Switching Paths, LSPs:

- E-LSP, where the QoS information is inferred from the EXP-field in the MPLS shim header.
- L-LSP, where the QoS information in part is inferred from the MPLS label.

In the E-LSP method, the DiffServ information is carried in the EXP-field in the MPLS shim header. This allows for 8 different QoS markings. Within the MPLS network the QoS marking is used to map to the DiffServ Per-Hop-Behaviour, PHB. This includes both the packet's scheduling treatment and the drop precedence. EXP to PHB mapping can either be explicitly signalled during LSP set-up or rely on a general pre-configured/default mapping.

In the L-LSP method, the DiffServ information is carried partly by the packet's associated label and partly in the EXP-field in the MPLS shim header. Within the MPLS network the QoS marking is used to decide the PHB. The associated label specifies the packet's scheduling treatment while the drop precedence is carried in the EXP-field.

Both E-LSPs and L-LSPs may be established with or without bandwidth reservations. The signalled bandwidth requirements may be used for admission control or for resource adjustment.

7.3.3.2 DiffServ aware MPLS

DiffServ aware MPLS traffic engineering (DS-TE) might be supported in networks, which have strong requirements on network resource utilization. DS-TE might impact scalability, but in small network with limited number of nodes this is not an issue. The only scalability concern might be due to instability of underlying transmission infrastructure or a large degree of site mobility.

These mechanisms should mainly be used if other TE mechanisms do not support the required resource control or within the most critical parts of the network.

7.3.3.3 Current status

Today, many router vendors support DiffServ MPLS. Management systems supporting traffic engineering operations are becoming available. These tools would be applicable for less dynamic networks like the strategic backbone and even deployable tactical networks, but are not targeted towards highly dynamic mobile networks.

7.3.4 Summary of QoS mechanisms and architectures

QoS mechanisms: **Properties:**	**DiffServ**	**IntServ w/RSVP**	**DS-TE**	**DiffServ-MPLS**
Current standardization & support	Available and is being deployed in commercial networks	Available, but not widely used	User standardization, not available	Available, but standards not finalized
Individual flow distinction	NO	YES	Aggregate per class	Aggregate per behaviour aggregate
Scalability	Highly scalable	Limited scalability in very high capacity networks	Scalable, but with limitations	Highly Scalable
Stateless	Minimal state	NO	NO	No, but minimal state
Typical granularity	Low: (4-8)	High: (1000-10 000)	2-4 (maybe more)	Typically 8, might support more
Aggregation support	Edge marking and classification possible	Possible (drafted)	YES	YES
Quantitative guarantees on throughput, delay and jitter on an end-to-end basis	NO	YES (Guaranteed Service)	To some extent	No
Qualitative performance	YES	YES	YES	YES
Management complexity	Easy	Complex	Complex	Easy
Dynamic admission control inherently supported	NO	Yes, on a per flow	Yes, on an aggregated level	Edge policing
Expected future standardization & support in commercial networks	YES	Only in edge routers	YES Core routers	YES Core routers
Expected future use in military networks	YES, in high bandwidth areas	YES, throughout the network with exception of ad hoc mobile networks	Possibly in strategic backbone networks	Possibly in strategic networks

The different QoS mechanisms are optimized for different networking scenarios and in a NCW network several of the mechanisms are likely to be deployed.

7.4 QoS management

Currently, Service Level Agreements (SLA) are used to define the service level delivered by the network and service operators. There is no common architecture that defines the functionality or API needed to define, monitor, control and take actions based on such SLAs. The use of SLAs in military networks have been proposed both to regulate the relationship between nations in coalition operations, but also as a mechanism to regulate traffic control inside a national network.

The Policy Systems are expected to control, provision and monitor the QoS mechanisms inside a network and the interfaces between different operator's networks. They will use SLA as a basis for this. In the future, the policy control systems are expected to be based on the QoS policy model [31] standardized by the IETF and DNTF (Distributed Management Task Force). Standards are emerging, and some very limited implementations are available, but this is currently not a mature technology.

The use of SLAs is still immature even in commercial networks and how to deploy them in military networks will require additional work as the operational environment differs with regard to enforcement of SLAs, but the use of SLAs and BB/PBQM are likely to be used to control the relationship between nations in coalition networks. It has been suggested by TACOMS as a mechanism to control the national network operations. It is also being experimented with in other coalition research projects like The Technical Cooperation Program (TTCP), which includes, US, Canada and Australia.

7.4.1 Policy Based QoS Management and Bandwidth Broker

The Policy Based QoS Network Management (PBQM) and Bandwidth Broker (BB) solutions are based on the establishment of a controlling entity that has access to information about the network topology, bandwidth usage and controls the QoS configuration of the network elements. This enables them to change the QoS configuration including the traffic classification and marking based upon events happening in the network or changes to the user configured QoS policies.

The architecture of Policy Based Networking (PBN) consists of two kinds of elements, Policy Decision Points (PDP), and Policy Enforcement Points (PEP) [32]. The basic interaction between the components begins with the PEP. The PEP will receive a notification or a message that requires a policy decision. Given such an event, the PEP then formulates a request for a policy decision and sends it to the PDP. PDP handles the request with the help of policy repository and returns the policy decision. PEP then enforces the policy decision [46].

Policies are stored in the policy repository. The central repository can be used to distribute and share the same policy information among multiple policy systems. Directories and LDAP are the choice for interoperable standard policy storage. The policies in the directory are typically at high level of abstraction and the policy system (i.e. PDP and PEP) translates them into the network node specific configurations.

BB and PBQM elements make it possible to allocate bandwidth for en-to-end connections without requiring that the every network element should hold the state information. The BB

architecture does not require multilateral agreements, but allows services to be build using multiple bilateral agreements between network operators. This is mainly a requirement from commercial operators and the bilateral relationship between the operators are detailed in Service Level Agreements (SLAs) specifying the service provisioning policies. The BB/PBQM architecture consists of the following functions:

- *User Interface*: The user/application interface provides a means for the user to make resource requests directly, or to the network operator who will enter his requests. The interface also receives messages from set-up protocols. Typically this interface may be based on RSVP or other lightweight signalling protocols.
- *Inter-domain Interactions*: A method of allowing peer BB's to make requests for resources and admission control decisions to enable flow of traffic.
- *Intra-domain Interactions*: Providing a method for the BB/PBQM to configure the edge routers within the domain so as to provide quality of service. IETF has standardized the COPS protocol [47] for communication between the policy decision point and the policy enforcement point.
- *Routing Table*: A routing table is maintained to access inter-domain routing information so that BB can determine the edge routers and the downstream routers before allocating their resources. Also additionally routing paths can be maintained for different flows within the domain.
- *Database*: Databases are used to store information about all the BB's parameters. The different information that is stored within the repository is: SLA's, current reservations, configuration of routers, DSCP mapping, and policy information.

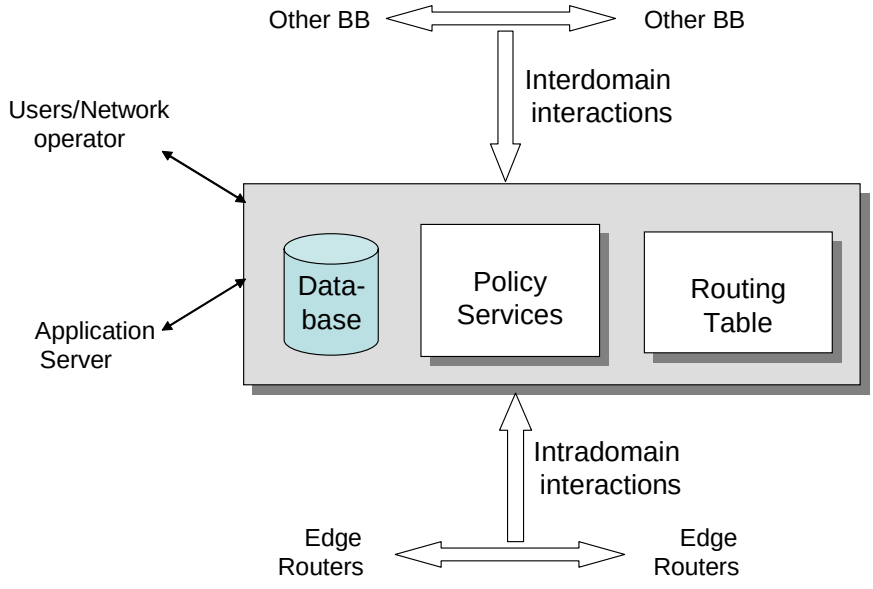

Figure 7-2: BB/PBQM functions

The BB/PBQM keeps track of current allocation of marked traffic, and interprets new requests to mark traffic in light of the policies and current allocation. It is associated with a particular QoS administration region/domain. It is responsible for allocating bandwidth for end-to-end connections using SLA-information and user defined policies, configure intradomain network nodes/router, decide internal and external admission control and negotiate with bandwidth brokers from neighbouring domains as shown in figure 7-3. The BB/PBQM will manage all DiffServ resources in an administratively defined domain and thus provide proper resources for flows.

The use of BB/PBQM internally in a national network may be used to control the borders between different network technologies, e.g. where requires a robust configuration of the BB/PBQM servers and decision components to ensure robust network operation during topology changes and network degradation. Since these types of elements have mainly been developed to regulate the relationship between operators interconnecting high capacity networks, little effort has been devoted to limit signalling overhead.

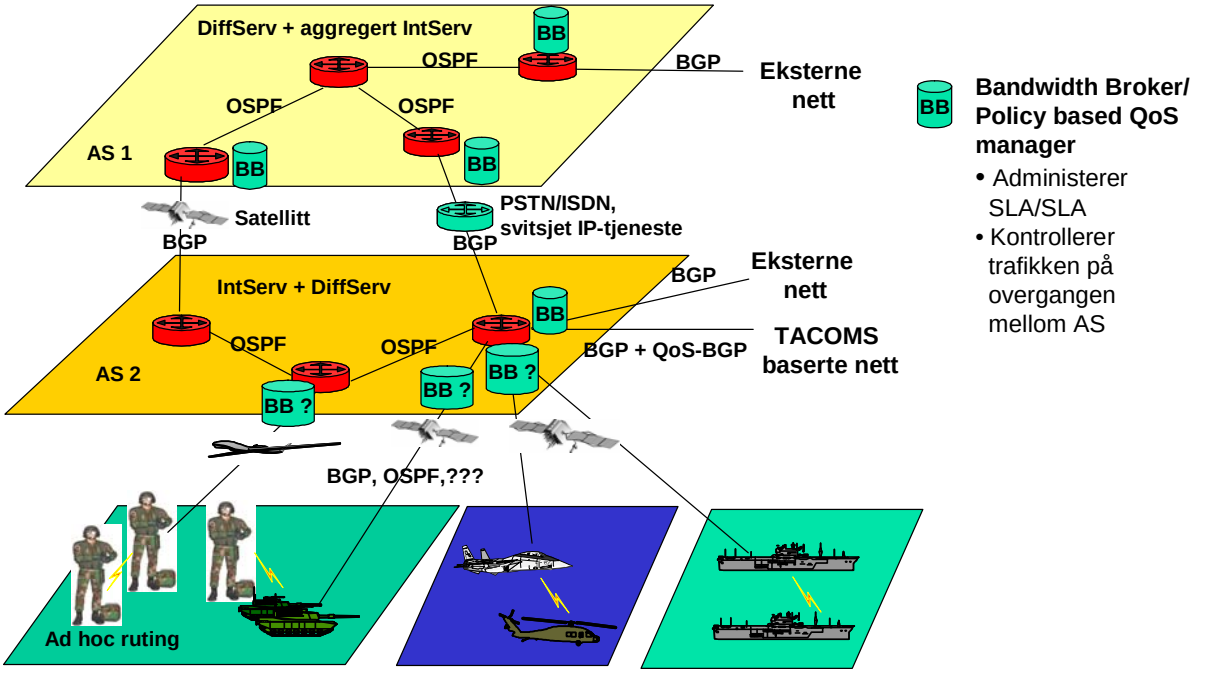

Figure 7-3: An example of use of different QoS mechanisms in a military network.

7.5 Recommendations and conclusions

Technologies for supporting differentiated service guarantees are currently offered by suppliers of COTS solutions, but not all system components are fully standardised and available and they do not fulfil all military requirements. The most commonly supported QoS mechanism is DiffServ with classification, marking, intelligent queuing and to a limited extent IntServ with RSVP signalling with policy control elements.

Currently available QoS mechanisms are probably sufficient to support service guarantees in relatively static networks with predictable network operation. This includes strategic networks and tactical operational networks deployed as part of for example peace-keeping missions. These types of networks consists of multiple QoS domains each offering a set of mechanisms,

e.g. IntServ or DiffServ, and needs to be augmented with a BB/PBQM solution to control traffic in and out of the different QoS domains. However, QoS mechanisms for mobile ad hoc networks are still immature and will required additional research, but the standardisation groups are working to solve these issues.

To limit the number of different QoS solutions that must be supported, it may be possible to use the same QoS architecture for all types of networks. The most favourable solution is then a combination of IntServ and DiffServ. IntServ is used in the edge networks and for services requiring stringent quality guarantees, whereas DiffServ and Aggregated RSVP are used in the core networks and over network tunnels, e.g. IPsec tunnels. Also the support of the DiffServ code points together with RSVP reservations will make it possible for network elements experiencing topology changes to use the DiffServ code point for traffic scheduling until the RSVP reservations have been restored and the network has reached stable working conditions. This solution is based on standardized components and offers a scalable and flexible QoS architecture.

The QoS management systems available have limited functionality and robustness. These systems are expected to evolve during the next years, but it is uncertain whether the COTS solutions will target all the military requirements. Implementation of policy based management does not alter the fact that to make viable and manageable QoS strategies and policies will require careful planning, detailed knowledge of traffic characteristics and an understanding of the QoS requirements based on the applications and operational needs.

As a first step the introduction of DiffServ and IntServ using static marking is possible and will increase the robustness in case of congestion even though a full support of multi-level priority and pre-emption cannot be supported. This does require a common strategy for traffic marking. Also all new applications with stringent quality requirements should support the use of both DiffServ marking and RSVP signalling.

As additional functionality becomes available, the use of more dynamic QoS management can be introduced, making it possible to more easily support changing networking and operating conditions. .

7.5.1 US DOD GIG QoS/CoS

The US DoD GIG QoS/COS working group has offered a roadmap for the introduction of QoS. In the first phase (2003-2005) static QoS marking is used to assure the quality for parts of the traffic like voice and video. In the second phase (2006-2008), policy based dynamic class of service with admission control will be introduced supporting multi-level priority and pre-emption for some applications, e.g. voice. In the third phase (2009-2011) all applications will support a fully dynamic mission dependent end-to-end user defined priority control.

This roadmap does not detail the mechanisms to be used unless for the first phase where a combination of DiffServ, MPLS-TE and static policy management is foreseen.

8 PUSH/PULL SERVICES

In the NCW model, data can be published (pushed) or subscribed to (pulled). In the former, the source publishes the data without knowledge of all the receivers. In the latter case, users of information can subscribe to data without a full knowledge of the particular source of data. Normally, push and pull are accompanying services, since one assume the other. Both alternatives can be found in standard COTS networks. Examples of push services are preloading of web caches, and TV distribution. Examples of pull services are video on demand, and TV viewing over the network. Push and pull services can be realized with different technologies. From a technology viewpoint the deciding factor is the real-time aspect of the data. Non real-time data is best produced over a Content Delivery Network (CDN) [2], which is an overlay network of specially adapted servers. Real-time data is best delivered through some sort of multicasting. The two architectures can be combined.

8.1 Non real-time service

8.1.1 Content Delivery Networks (CDN)

CDN is a broad class of overlay network with specialized servers for distribution of information. At one of the scale is web caches where the functionality is geared towards load distribution and preloading of interesting information. The other end of the scale is geared towards distribution of multimedia where there are specialized servers for registering, storing, locating, and distributing objects [2].

From an architectural viewpoint the following conclusions can be made:

If non real-time data is subject to a push/pull service, a CDN must be implemented. The CDN network will be a function of the non real-time information that is subject to the push/pull service. It cannot be designed before the information is described in more detail. If the web service paradigm is chosen, a web caching structure is the natural choice.

CDN can be added without requiring significant changes to the underlying network. A multimedia oriented CDN is an overlay network with a separate API added to the terminals. From the IP network it will appear as a set of servers. It can therefore be added later without any additional changes to the underlying IP network. A CDN based on a web caching approach is not as transparent, since intercept and redirection of http requests are a fundamental part of the mechanism. However, retrofitting the use of web proxies into functioning IP network is of limited complexity. Once the use of proxies are in place, a web based CDN can be added requiring some changes in the proxies.

Push/pull services for non-real time data distribution can be added at any time without requiring major changes to the underlying network. The architecture of the non real-time services should reflect the type of data. It should therefore be fixed once it is known what kinds of information that will be distributed.

8.2 Real-time services

Real-time data distribution, or streaming, is typically done through multicasting. Multicasting is based on a distribution tree where packets are copied a close as possible to the destination. At any link in the distribution tree, only one copy of a packet will be transmitted. Compared to unicasting, multicasting saves resources on the transmission links, in the sources, and in the routers. The cost is in maintaining the distribution trees.

8.2.1 IP multicast model

Multicast has been a part of Internet since 1992 [3], and the dominant protocols can be found in most routers. Multicast sessions use a separate class of IP addresses, class D. The address space is flat, with a few pre-allocated addresses. The addresses can be scoped (in particular in IPv6), to limit multicast distribution to a logical unit, like organization, company, or campus.

The IP multicast model assumes [3]:

- The sources need not be member of a group. Sources can dynamically join or leave sessions.
- Receivers can dynamically join or leave a session. The sources will not know the receivers in a session.
- The receivers need not know the sources in a session.

For push/pull services such a model fits perfectly. However in a commercial environment it has several weaknesses [3]. The lack of group control hinders usage billing. From a source perspective it is difficult to protect content and to build brand loyalty; Addresses are not fixed, and there are no mechanisms to block externals from injecting new content into a session [3]. However this is not an issue in closed network like the NCW network where all sources are under the same administrative control.

8.2.2 Alternative multicast architectures

Multicast distribution can be classified into three groups, shared distribution trees, source specific trees, and connectionless multicast.

8.2.2.1 Shared tree

In shared trees, all sources use the same distribution tree. Shared trees will typically minimize the total number of links, but at the cost of longer delay and concentration of traffic to a fewer links. Shared trees match the push/pull model the best, since the receivers just subscribe to a session and not the individual sources. With shared trees there is no need to discover potential sources for data; the sources are discovered when the first packet is delivered.

In the dominant shared tree protocols, the trees are constructed based on a common node. The common node is a single point of failure. It can be made robust by different methods. The common feature is to use several common nodes, and either elect the one that should be used or use separate common trees and exchange data between them. The dominant shared tree

protocol is protocol independent multicast sparse mode (PIM-SM [4]). Most router vendors implement it.

8.2.2.2 Source specific trees

The alternative to shared trees is to build source specific trees to each source. It will minimize the delay to each source, but at the cost of larger number of links used and larger state space in the routers. The disadvantage with source specific trees is the source discovery. It assumes that the sources are posted at web sites or that they are pre-configured. The mechanism to subscribe to source specific trees has been standardized in version 3 of the IGMP protocol [7]. Source specific multicast, SSM, is the dominant protocol [38]. Its basis is a subset of PIM-SM. PIM-SM and SSM should be able to operate concurrently in the same network.

In limited environments, where most of the nodes are interested in information, a flooding version of source specific multicast can be used. With protocol independent multicast, dense mode, a source floods periodically data packets to all nodes in the system. Those nodes that are not interested unsubscribe to the distribution. Until the next flooding, the source distributes only to those nodes that did not unsubscribe. The scheme is only suitable in limited environment, with available bandwidth and where most nodes potentially are interested. The advantage is that the receivers need not know the source in advance. They only need to unsubscribe to the sources in a session they are not interested in.

8.2.2.3 Connectionless multicast

The third alternative is connectionless multicast, where no distribution tree is built. Instead, each packet contains a full distribution list [9]. At each router, the distribution list is evaluated and a copy of the packet with a modified distribution list is sent on links that are on the shortest path to the members of the distribution list. The protocols are aimed at small sessions where most of the hops in the distribution tree will have one incoming link and one outgoing. The connectionless protocols avoid the overhead of maintaining a distribution tree that contains long chains of unicast paths while avoiding sending multiple copies over bottleneck links. The cost is more processing of each packet and a limited number of receivers that can be supported. The connectionless protocols assume that the sources have full knowledge of all receivers and an additional signalling protocol for subscribing and cancelling interest in data will be required. The connectionless protocols are neither standardized nor widely implemented.

8.3 Analysis

The dominant shared tree protocol can switch over to source specific distribution trees. The default configuration is to do so when the first packet from a source arrives. It combines the advantages of both shared and source specific trees. It allows the receivers to discover new sources through the shared tree. However, the vulnerability of the shared tree is avoided for most of the data distribution. The cost is a more complex protocol implementation. PIM-SM is

a soft state protocol, and as such fairly robust. The vulnerability of the shared tree during the discovery phase can be alleviated by any one of the three commonly used alternatives.

In a COTS environment, the disadvantage of PIM SM is the lack of group and address control [3]. However it is a close match to the requirements in the push/pull data distribution model for real-time data. In a COTS environment the concerns are related to billing, content control, and branding. In a strictly controlled NCW environment these issue are of less concern.

8.4 Recommendations

We recommend that multicast is used for push/pull real-time data distribution. PIM-SM with automatic switchover is suitable when there are multiple sources and/or when the sources are not known in advances. Implementations of PIM-SM are readily available, and well tested. However, the distribution across administrative domains is slow. Source specific multicast (SSM) is recommended for data sources that are well known and potentially located in a different domain.

8.5 Open Issues

Although multicast has been available for more than a decade there are several unresolved issues. In the COTS environment, there is substantial focus on session address allocation. However in a NCW environment, this is not an issue, since the same administrative domain can allocate all addresses. Instead, there need to be additional focus on robustness, QoS, interdomain distribution. An additional issue is reliable multicast. This will not be discussed, since the meaning of reliable transfer in a push/pull model is unclear. Reliable multicast can be implemented as an overlay network. It is therefore not a crucial part of the initial architecture.

8.5.1 Robustness

In multicast, a loop in the distribution tree will result in exponential increase in workload. Protocols will therefore typically use a reversed path forwarding (RPF) check to avoid such situations. With RPF, a router will not forward a multicast packet unless it is received on the interface that is on the routing path towards the source. The disadvantage is a lack of robustness and inability to handle fast rerouting. In a NCW network these properties needs to emphasized, and different algorithms for building distribution trees should be developed.

8.5.2 QoS

The distribution trees are currently built based on shortest path routing. If the receivers have different QoS requirements other strategies for building the trees need to be investigated.

8.5.3 Inter domain distribution

PIM-SM is an intradomain protocol, since the common node to build the shared tree from should be placed within the domain. The common node needs to be configured into all edge routers and it should therefore be under the same administrative control as the edge nodes. In

addition, the shared tree needs to be reasonably close to the sources and receivers in order to be efficient. PIM-SM is accompanied by a multicast source discovery protocol (MSDP) for interdomain distribution. MSDP builds a source distribution network between dedicated servers. These servers distribute data packets from new interdomain sources into each intradomain shared tree. From there on, the regular source specific mechanisms are used.

In a dynamic environment with changing topology, this is not sufficient. In addition, MSDP is slow (adds substantial delay to the first packet) and not suited for bursty and short-lived sessions [3], [8]. In a NCW environment are more suitable mechanism needs to be developed.

9 INTERFACE TO EXTERNAL NETWORKS AND INTERNATIONAL INITIATIVES

Military NCW networks are likely to interconnect to two main types of network, other military network and commercial networks.

Interconnection of different operators/organizations IP networks are normally supported using either a peering relation where the two operators are considered to operate at equal terms making services available to each other, or a provider relation where one operator is offering a service to the other. A third type is Internet access, but this is not discussed here.

Interconnections to other military networks can use both schemes. The TACOMS standardized solution is an example of a peering relation for military networks, see chapter 9.3. By standardizing addressing structure, routing, service and mobility handling and user and service location mechanisms, there will be no need for bilateral agreements.

9.1 Provider relation

In the case where a provider (commercial operator or other military operator) offers a network service to a user or customer, this can be characterized as a provider relation. Normally this can be done using different technologies, but we only discuss the use of operator administrated IP based services offering a controlled quality.

Provider controlled IP services are normally offered through IP based VPN services. This makes it possible to multiplex/overlay traffic from multiple users/customers over a single IP network. Since the provider network routing and customer routing are kept separate, there is no need for coordination of the network addressing or routing architectures. This makes it possible for the customer private IP addresses and customer border does not need to align with for example an AS border or OSPF area border.

Communication between the different VPN users/customers are limited, but can be provided by opening up the VPNs allowing communication to others via a firewall and/or NAT (Network Address Translator) devices.

A Service Relation Agreement specifying the service quality guarantees and operational aspects of the service normally regulates a customer-provider relation. Use of IP based VPNs are useful when buying services from commercial operators, but may also be used to offer

communication services to other coalition nations if the main purpose is to provide transit communication and the need for communication between different users is very limited.

9.2 Peering relation

Peering agreements require stronger coordination between the interconnecting parties since both the addressing and routing architectures must be aligned. The BGP interdomain routing protocol is used to support interconnection of different administrative domains (operator networks). The protocol assures global connectivity and it allows both peering parties to define their own policies to control the traffic in and out of their network.

A traditional peering relation is assumed to support equal partners where each offers a service to the other. As the commercialisation of the Internet has matured, large providers charge unequal peering partners based on the difference in benefit, this means that operators with small networks and limited capacity must pay to peer with larger providers since the customers of the small providers are likely to generate more traffic into the large providers' networks than vice versa. In a military environment, the peering relationships are not governed by commercial principles.

The current peering mechanisms (BGP) only offer interdomain connectivity. In the commercial environment, this favours large operators since limited interdomain functionality makes it more attractive to be a customer of a large operator since they can offer more functionality rich services over larger geographical areas. The result has been low interest in developing solutions for interdomain services and therefore little effort is been spent in the standardization bodies defining mechanisms and protocols to support for example mobility, QoS services, multicast, VPNs and security across interdomain interfaces.

Peering is a very flexible method requiring a minimum of operational and administrative coordination to interconnect coalition partners' networks and military networks with different characteristics, for example mobile tactical networks and deployable tactical networks since they use different routing protocols. However, the lack of standardization makes it difficult to support the military requirements across standardized interdomain interfaces. It will require additional developments to support a flexible network architecture for NCW operations.

9.3 TACOMS

The TACOMS specifications are focusing on defining the interoperability standards for interconnection of different nations' network elements (NE). The TACOMS model is based on a peering-like relation, but extended to include support for services currently not standardized for inter-domain operation. In addition it specifies military specific requirements and services that need to be supported.

Different types of network elements are identified, LAS (Local Area Systems), WAS (Wide Area Systems), RAPNET (Radio Access Packet Network) and two types of MS (Mobile Area Systems), PNET (Packet Network) and CNET (Circuit Network). The different network elements are interconnected over a set of InterOperability Point (IOP). Figure 9-1 shows the possible interconnection of NEs in a TACOMS compatible network infrastructure.

The national NE may use different networking technologies, e.g. IP, TDM, ATM, etc. To ensure interoperability TACOMS specifies a service interface for connection less data and connection oriented data (real time voice and video), an addressing structure, mobility functions, a service quality regime, inter-NE routing protocols for both CO and CL traffic, security architectures for both traffic classes and interfaces towards external networks.

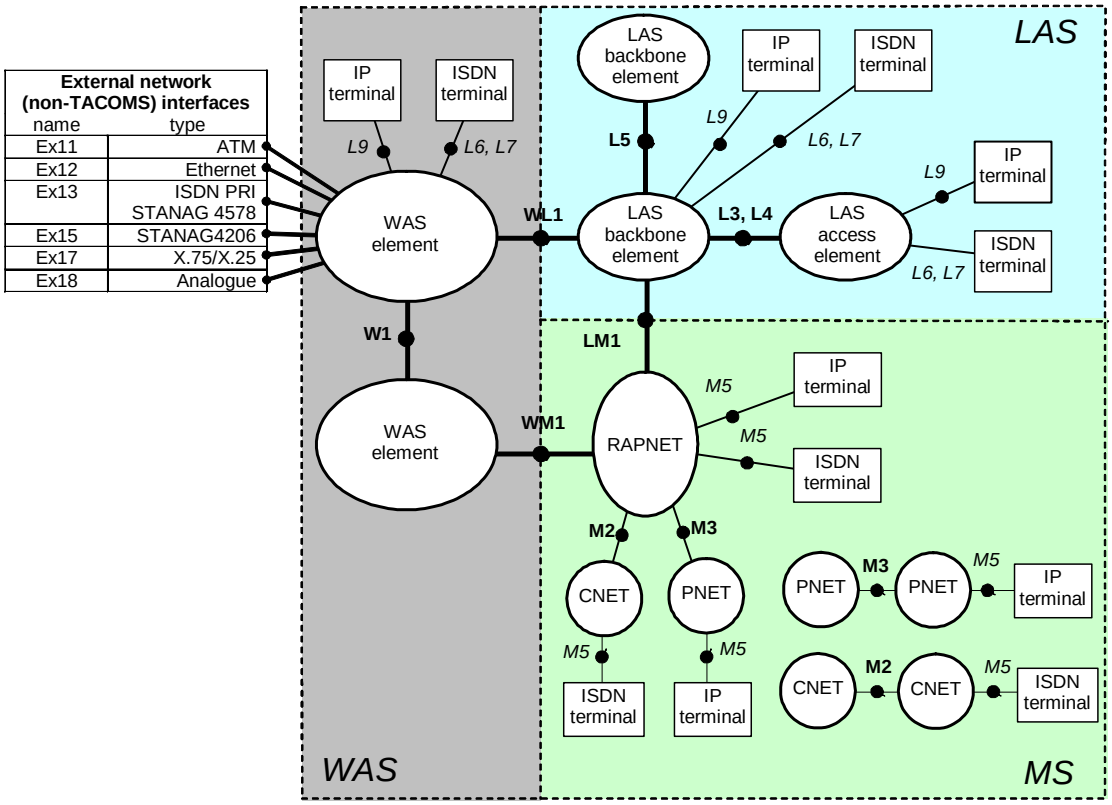

Figure 9-1: TACOMS network architecture

9.3.1 Directory and mobility handling

All TACOMS terminals are identified by IP addresses and the battlefield directory system maps between usernames/services and IP addresses. The battlefield directory is also used to support user mobility between TACOMS network elements. When users move and re-affiliate, they will obtain a new IP address from the local address space and must register themselves with this new address in the directory. The directory service through its replication mechanisms distributes the information across the TACOMS network. For TACOMS networks operating at different security levels, one battlefield directory is required for each security level.

9.3.2 Traffic handling

The physical interface between TACOMS network elements (IOP) is based on the use of IP over MPLS over Ethernet. MPLS is used to differentiate between the traffic classes. TACOMS specifies two main types of traffic classes, connection oriented (CO) and connection less (CL).

Service Level Agreements (SLA) will detail the service requirements of the national network elements in terms of traffic classes supported, throughput/bandwidth and delay. The CO traffic includes real-time traffic like voice and video and the CL traffic includes all other data traffic. These two traffic classes are transported over different MPLS label switched paths (LSP) to secure that the requested quality of service is provided. The connection less traffic offers additional traffic classes through use of standard DiffServ mechanisms. While the CO traffic is handled using DiffServ with the addition of admission control functions located at the NE entry points.

The CL traffic is routed and forwarded using standard Internet protocols. BGP4 is the main interdomain routing protocol chosen for routing between NEs. OSPF may be used in some cases, for example when interconnecting packet switched mobile radio networks.

The real-time CO traffic will use H.323 with extensions to support priority (this is defined in H.323 version 5. Whether other military extensions are to be supported is not clear. The CO signalling will establish connections through the TACOMS network and the CO traffic will be forwarded along this path.

The connection oriented traffic is routed using a dedicated CO routing protocol, which is based on BGP4, but extended with additional mechanisms to support routing based on quality parameters like delay and bandwidth and possibly other network and service capabilities. In addition a flooding mechanism is suggested as an additional mechanism to ensure that the high priority traffic is provided a route even when a route with sufficient resources is not found by the BGP4-like routing protocol.

It is not exactly clear how the two traffic classes must be handled internally in the NE since the NE internal traffic handling requirements have not been fully specified. The impacts of the TACOMS specifications in this area are therefore difficult to predict. For example the most likely case is that the CO traffic must be supported by QoS mechanisms ensuring a service quality fulfilling the service specifications outlined in an operational SLA (Service Level Agreement) and that the traffic must be supported by mechanisms which ensure that the NE entry and exit points are fixed through the lifetime of the a CO session.

9.3.3 Security architecture

The TACOMS security architecture is based on a combination of edge-to-edge and end-to-end encryption. The voice traffic that is based on the use of the FNBDT-standard will support end-to-end encryption over a NATO restricted or unclassified network. The remaining traffic will be protected using edge encryption based on the IPsec tunnelling mode. These two security solutions imply the existence of two logical networks, one NATO restricted for the voice traffic and one for the remaining traffic. For FNBDT terminals located inside a NATO secret domain special security bypass functionality is required since the FNBDT traffic cannot go via the edge crypto. The same is needed for directory information to be able to locate the users in different security domains.

It is unclear how non-FNBDT voice and real-time video will be handled since these are defined as CO-traffic and are handled by a different set of mechanisms compared to the CL-traffic.

9.3.4 Impact on Network Centric Warfare

The TACOMS specifications will be draft proposals and will have to go through several revisions before reaching a steady state. This makes it difficult to predict the final result in terms of NATO STANAGs.

The most controversial decisions are probably the definition of CL and CO traffic, even though the distinctions between the two are becoming less clear. The reason for having this division is mainly due to the lack of confidence in the IP QoS mechanisms to secure the service quality for real-time traffic. The main argument against this division into CO and CL is that there are some underlying assumptions that the CO traffic, i.e. only the voice and video traffic, has stringent service qualities. This may not be the case, as weapon systems connected to the network and requires communication with sensors and remote control units. It is likely that these will have at least if not even more stringent service quality requirements. With the current definition of CO and CL, these kinds of applications are not easily handled. There are several problems:

- Firstly, there are no mechanisms defined to support signalling of resource reservation across an IOP for the CL traffic and only H.323 is available for the CO traffic. This may limit the possibilities for non-voice/video application with stringent delay and bandwidth requirements to be ensured a sufficient service quality. To use the CO service, they need to use H.323 signalling which have limited QoS signalling capabilities.
- Secondly, the use of H.323 for resource signalling requires the use of H.323 call handlers at all ingress boundaries to implement call admission.
- Thirdly, CO group communication will use conference bridges. This implies that also data traffic will have to be treated by a conference bridge.
- Fourthly, there are no ways to differentiate between different users of the data. In an NCW context it is assumed that importance of data and service quality of the data can be targeted towards the different user’s needs. This implies that information may be treated as real-time traffic for some users while not time-critical for other users. This is difficult to achieve without requiring that the applications are capable of supporting both traffic handling classes.

The CO traffic handling is also supported by a separate routing function allowing CO traffic to be routed differently through the network compared to the CL traffic and the CO traffic being connection oriented must follow the same path through the network for the duration of the call. In TACOMS terms this means that the entry and exit point of a Network Element must be the same. The internal operation of the NE does not need to be connection oriented as long as the entry and exit points do not change. This means that if the there is a route change causing a change in for example a NE’s exit point, the call will be terminated instead of rerouted. For NEs not supporting a connection oriented type of service, this must be mirrored either through the use of tunnelling, where the tunnel end-point corresponds to the NE exit point or the use of source routing if not the calls are likely to be terminated as a result of changes in the internal NE topology even though the network is capable of supporting the call. The impact of this for

highly mobile networks where the routing and attachment to external networks changes frequently is uncertain, but may result in more frequent termination of calls.

It has been stated that as soon as the underlying networks are capable of supporting the service requirements of the CO traffic using the QoS mechanisms defined for the CL traffic, i.e. Internet based QoS mechanisms; it is possible for nations to decide to only support the CL traffic classed. The main problem with this is that as long as the CL traffic classes are not designed to support the QoS requirements of real-time voice and video services, they will not necessarily support the most optimal QoS mechanisms for this kind of traffic. Since only DiffServ is supported with no per flow resource signalling, an end-to-end resource signalling across a TACOMS network can not be supported and the NEs will either have to mirror the TACOMS DiffServ regime or try and make assumptions about the traffic requirements of particular traffic flows. One possible solution is to use RSVP, since RSVP does not have to be supported by all network nodes, but the signalling messages must be forwarded by all network elements.

The use of a common battlefield directory system to support user mobility will require a connection to the NE internal mobility handling. The complexity of this depends on how mobility is handled inside the NE. The simplest case is probably where Mobile IP is used inside the NE. This will not require updates in the battlefield directory whenever users move inside the NE, since the mobile terminal is reachable via its original IP address. It is not known by the other TACOMS users that the traffic is routed via the Home Agent. Use of other mobility schemes may require updates in the battlefield directory also when users move inside the NE. Depending on the update and replication mechanisms this may lead to substantial overhead traffic since NCW operation assumes a higher degree of mobility compared to existing operational practise.

9.3.5 Impact on national networks

The impact of the TACOMS proposals to the national networks are not clear and there is currently no ongoing work within TACOMS to summarize all requirement towards the national networks as these will vary depending on the structure, technologies and mechanisms supported by the different national networks. It will be left to the different nations to take the TACOMS requirements into their national network specifications and designs in order to be TACOMS compatible. The added cost of upgrading existing networks will vary depending on the functionality supported and technology used in existing national networks. Migration of existing networks to offer TACOMS compliant functionality may prove to be very expensive in some cases while in other cases it is relatively simple. It may be and important cost factor when making decisions on continued upgrade of existing systems versus deploying new technology.

10 VOICE

In a NCW network architecture, voice is one of many services that must be carried. In this section we discuss the need of integrating voice and data and the implication it will have.

There are three alternatives. Voice and data can be carried in two separate networks, they can be carried in two virtual networks that are multiplexed onto the same physical network, and voice and data can be integrated into the same IP network. In the next paragraphs the advantages and disadvantages will be outlined.

10.1 Separate networks

Under this alternative two separate transmission and switching systems need to be installed, maintained, and administrated. Obviously there is no multiplexing effect and the efficiency is therefore less.

10.2 Two virtual networks carried over the same network

In the virtual network architecture the transmission links are shared. However, in addition to the multiplexing equipment, two separate switching systems need to be installed, maintained, and administrated. The topology is limited by requiring having both types of switching systems at every interconnection point. The alternative is to add switching in the multiplexing equipment.

The multiplexing will have limited dynamic properties unless switched ATM is used as the multiplexing technology. Voice and data will therefore operate under different priority regimes. It will therefore be situations were voice calls are blocked, while low priority data is being transmitted and visa versa.

Ad hoc networking is likely to be an important part of NCW networks. Link layer multiplexing techniques for this scenario requires additional focus.

10.3 One integrated network

The dynamic priority assignment required in NCW implies that voice should be considered one out of many services, where priority can change. The architecture minimizes the type and amount of switching equipment that needs to be installed, maintained, and administrated. Voice does not represent any fundamental difference in QoS requirement compared to other serves that the IP network must carry. Routers do not impose any fundamental limiting processes for transmission of voice. The delay is of the other magnitude smaller than the acceptable end-to-end delay. However, the small packets in voice over IP impose limitation in the carrying capacity for some technologies. However, the issues are the same for any data application with short packets.

10.4 Implications

In the final NCW voice should be an integrated part of the network. The lack of flexibility and cost in terms of administration and maintenance will prohibit other alternatives. However voice carried over IP adds some additional restriction in terms of performance over wireless technologies.

Standard link layers use CRC to detect bit errors in the packet. To avoid misdirection of packets and minimize application processing, corrupted packets are normally discarded. Over wireless technologies, the effect of bit errors is therefore amplified. This is not a fundamental part of the IP protocol, but represents a universally accepted trade-off between performance and robustness.

Traditionally, voice and data have used different routing strategies. For example in TADKOM flooding is used to find an available path. This is to ensure that if there is an available path, the call will be set up. This is done at the cost of overhead and potentially decreasing the carrying capacity of the whole network. In TADKOM there are no mechanisms for protecting ongoing calls against link and switch errors.

In IP different properties have been optimised. The focus is on rerouting ongoing flows in response to link and router errors. Typically shortest path is used, and unless load-sharing techniques are used, a call may be blocked even though a path exists with available resources.

The optimal strategy in terms of carrying capacity depends on the topology of the network. In ad hoc networks based on omni directional antennas and in wireline networks with sparse topology, utilizing all possible paths is counterproductive. In network with a high degree of interconnection is can improve the carrying capacity. The flooding based voice routing is therefore not dominant over the routing typically used in IP networks.

Wireless LAN based on IEEE 802.11b standards is gaining popularity in the COTS networks. An 802.11b network has a gross bandwidth of 11 Mb/s, unfortunately the protocol was designed for large packet, and the overhead for small packets is substantial. The total carrying capacity for 64 kbps voice with 10 ms sampling is 6 calls per cell [11]. The capacity is mainly determined by the number of packets. Lower bandwidth codecs will improve the capacity to a small degree, while lengthening the sampling will have a better effect. If wireless LAN based on 802.11 technology is to be used, care need to be taken when it comes to dimensioning and structuring the networks.

10.4.1 FNBDT and signalling

The Future Narrow Band Digital Terminal, (FNBDT) defines a secure interoperable architecture that is independent of the underlying network technology. FNBDT is a collection of interoperability protocols enabling end-to-end secure, seamless voice and data communications across a heterogeneous communications infrastructure. FNBDT uses application layer signalling inserted into the reliable data transport capability of any network endpoint. This application layer signalling allows for a consistent format for FNBDT voice and data traffic overlaid on the bearer transport services through appropriate interworking functions.

The minimum essential requirement of the bearer to support end-to-end interoperable FNBDT communications is the capability of establishing a 2.4 kb/s data channel between the end terminals, (required to accommodate the STANAG-4591 voice coding algorithm). This could be a synchronous channel with exactly 2400 bps or an asynchronous channel. Another important point is that any secure applications, be it voice, data or video can be established, as long as the underlying network bearers can support the bandwidth.

The security architecture of FNBDT is fundamentally different to the edge-to-edge security architecture imposed by IPsec, where terminals need to be connected to a network at the same security level to be allowed to communicate. This makes it difficult to support both within the same logical network without introducing gateways allowing the FNBDT traffic to bypass the IPsec encryption device.

11 MIGRATION TO IPV6

A network architecture study must include a discussion of the IP dialect to use, IPv4 vs. IPv6. However, this is not a crucial issue. IETF has standardized IPv6 [16], which is a completely new protocol and is not backward compatible with IPv4 but intended to replace IPv4. IPv6 offers much needed enhancements to the IPv4 standards and can scale to accommodate the continued growth of IP based networks.

This includes larger address space and improved security, mobility and auto-configuration functionality. IPv4 can be enhanced to offer some of these functions, but the results are likely to be less useful than what could be obtained by widespread deployment of IPv6. The main contribution of IPv6 will be the increased address space. This will make it easier to support peer-to-peer services as terminals may have unique IP addresses instead of being accessible through a NAT (Network Address Translator) that maps between a few official addresses and private addresses used within the enterprise network. Also as more devices become network enabled, for examples sensors, this will increase the need for more IP addresses.

IPv6 products have been on the market for some time, but they do not offer the full functionality of IPv4 and network management and support systems have not been upgraded to support IPv6. The first commercial IPv6 services have been launched, but currently the use of IPv6 has had limited success outside Asia, where the lack of IP addresses are more profound, and to academic environments where the protocol has been used in research activities. Experiences from the INSC-project also showed that the IPv6 protocol functionalities are immature particularly in the area of network management and only a limited number of applications are available. Also more interoperability problems between vendors are experienced when using IPv6 resulting in the need to reach common agreements on vendor specific solutions.

To preserve existing investments in infrastructure and services IETF has standardized different transition mechanisms to support both interworking between and collocation of IPv4 and IPv6.

The main reason for deploying IPv6 is the need for a larger IP address space to accommodate an increased number of terminals and devices connected to the network. Also the improved mobility handling is interesting as it reduced the traffic in the network, which is especially important in low bandwidth military networks.

A migration to IPv6 is a long-term activity since existing applications and services need to be upgraded. Therefore, transition mechanisms are needed to ensure connectivity over IPv4 networks and interoperability with existing IPv4 hosts and applications. IETF has standardized different transition mechanisms to support different migration scenarios, leaving it to the

network operators and enterprises to decide when and how the migration towards IPv6 should be conducted.

11.1 US DoD IPv6 initiatives

The US DoD announced in June 2003, that migration to IPv6 is assumed be conducted in 2008 and this requires that all new procurements as of October 2003 must be IPv6 capable. There is however some exceptions, if IPv6 compatibility does not show a positive business case this requirement may be omitted. Therefore, it is difficult to determine the impact of this announcement, but it may be a turning point in the IPv6 deployment as this may force particularly the US vendors to speed up their IPv6 developments.

11.2 Recommendations

There is no immediate need to migrate to IPv6 since address limitations are currently not a problem for the Norwegian Defence. Introduction of IPv6 would increase the risk of network and service instability and as many applications are not available for IPv6 there would be a need to support both IPv4 and IPv6. The introduction of dual stack network will increase the network management burdens and result in increased administration and maintenance costs.

As the deployment of IPv6 gains momentum and applications and services become available, the risks of introducing IPv6 are reduced. This in combination with a possible increased need for IP addresses and the use of IPv6 by our coalition partners are likely to be the drivers for a migration to IPv6. This is likely to still be a few years ahead and is not considered a prioritised task at the moment.

However, a NCW network will have to interact with both IPv4 and IPv6 networks and terminals, either national or international IPv4 legacy systems or future international IPv6 systems. A dual stack and/or interworking units will therefore have to be included in the NCW network.

IPv6 support should be considered a requirement for new applications being developed since the added cost is very small when implementing IPv6 support in new applications compared to adding IPv6 at a later time.

12 REFERENCES

[1] Thierry Ernst, ed., *Network Mobility Support Goals and Requirements*, Internet-Draft: <draft-ietf-nemo-requirements-01.txt>, May 2003.

[2] H.D.Cranor, et al., *Enhanced Streaming Services in a content Distribution Network*, IEEE Internet Computing, 2001(July/August 2001): p. 66-74.

[3] C. Diot, et al., *Deployment issues for the IP multicast services and architecture.* IEEE Network, 2000(January/February): p. 78-88.

[4] D. Estrin, et al., *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification*, RFC 2362, 1998.

[5] B. Fenner, et al., *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*, Internet Draft: <draft-ietf-pim-sm-v2-new-08.txt>, 2003.

[6] W. Fenner, *Internet Group Management Protocol, V2*. 1997.

[7] B. Cain, et al., *Internet Group Management Protocol, Version 3,* RFC 3376, 2002.

[8] B. Fenner, Ed., D. Meyer, Ed., Multicast Source Discovery Protocol, RFC 3618, 2003.

[9] D. Ooms, W. Livens, and O. Paridaens, *Connectionless Multicast*. 2000.

[10] K. Almeroth, *The evolution of Multicast: From the Mbone to Interdomain multicast to Internet2 Deployment*, IEEE Network, (January/February) 2000: p. 10-20.

[11] F. Anjum, et al., *Voice Performance in WLAN Networks—An Experimental Study*, Globecom 2003, San Francisco, 2003.

[12] X. Hong, K. Xu, and Mario Gerla, *Scalable Routing Protocols for Mobile Ad Hoc Networks*, IEEE Network, 2002.

[13] M. Mauve and J. Widmer, *A survey on position-based Routing in Mobile Ad Hoc Networks.* IEEE Network, November/December 2001: p. 30-39.

[14] C. Tschudin and R. Gold, *LUNAR, Lightweight Underlay Network Ad-Hoc Routing*, Submitted, 2002.

[15] U. Varshney, *The status and future of 802.11-based WLANs*, IEEE Computer, 2003: 36(6): p. 102-105.

[16] S. Deering, R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification*, RFC 2460.

[17] C. Perkins, Editor. *IP Mobility Support*, RFC 2002, October 1996.

[18] A. Williams, *Requirements for Automatic Configuration of IP Hosts*, Internet-Draft: <draft-ietf-zeroconf-reqts-12.txt>, Sept 2002.

[19] S. Blake, et al., *An Architecture for Differentiated Services*, RFC 2475, December 1998.

[20] B. Davie, et al., *An Expedited Forwarding PHB (Per-Hop Behavior)*, RFC 3246, March 2000.

[21] J. Heinanen, et al., *Assured Forwarding PHB Group*, RFC 2597, June 1999.

[22] R. Braden, D. Clark, S. Shenker, *Integrated Services in the Internet Architecture*, RFC 1633, 1994.

[23] R. Braden, L. Zhang, S. Berson. S. Herzog, S. Jamin, *Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification*, RFC 2205, 1997.

[24] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, *An Architecture for Differentiated Services*, RFC 2475, 1998.

[25] K. Nichols, et al., *Definition of the Differentiated Services Field (DS-Field) in the IPv4 and IPv6 Headers*, RFC 2474, 1998.

[26] K. Ramakrishnan, S. Floyd, D. Black, *The Addition of Explicit Congestion Notification (ECN) to IP*, RFC 3168, 2001.

[27] A. Terzis, J. Krawczyk, J. Wroclawski, L. Zhang, *RSVP Operation Over IP Tunnels*, RFC 2746, 2000.

[28] E. Rosen, A. Viswanathan, R. Callon, *Multiprotocol Label Switching Architecture*, RFC 3031, 2001.

[29] F. Le Faucheur, Ed., *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*, RFC 3270, 2000.

[30] D. Awduche, et al., *Overview and Principles of Internet Traffic Engineering*, RFC 3272, 2002.

[31] Y. Snir, et al., *Policy Quality of Service (QoS) Information Model*, RFC 3644, 2003.

[32] A. Westerinen, et al., *Terminology for Policy-Based Management*, RFC 3198, 2001.

[33] R. Droms, *Dynamic Host Configuration Protocol*, RFC 2131, 1997.

[34] P. Mockapetris, *Domain Names – Implementation and Specification*, RFC 1035, 1987.

[35] P. Calhoun, et al., *Diameter Base Protocol*, RFC 3588, 2003.

[36] S. Thomson, T. Narten, *IPv6 Stateless Address Autoconfiguration*, RFC 2462, 1998.

[37] J. Hodges, R. Morgan, *Lightweight Directory Access Protocol (v3): Technical Specification*, RFC 3377, 2002.

[38] S. Bhattacharyya, Ed., An Overview of Source-Specific Multicast (SSM), RFC 3569, 2003.

[39] D. Clark, *The Design Philosophy of the DARPA Internet protocols*, Proc SIGCOMM 1988, Sept 1988.

[40] A. Terzis, J. Krawczyk, J. Wroclawski and L. Zhang, *RSVP Operation Over IP Tunnels*, RFC 2746, January 2000.

[41] L. Berger and T. O'Malley, *RSVP Extensions for IPSEC Data Flows*, RFC 2207, 1997.

[42] F. Baker, C. Iturralde, F. Le Faucheur and B. Davie, *Aggregation of RSVP for IPv4 and IPv6 Reservations*, RFC 3175, September 2001.

[43] Øivind Kure, Ingvild Sorteberg, Knut Øvsthus, *Architecture for TDM Circuit Emulation over IP in Tactical Networks*, Milcom 2003.

[44] F. Baker, *MLEF Considered Harmful*, <draft-baker-tsvwg-mlef-concerns-00>, December 2003.

[45] F. Baker, *Implementing MLPP in the Internet Protocol Suite*, <draft-baker-tsvwg-mlpp-that-works-00>, December 2003.

[46] R. Yavatkar, D. Pendarakis, R. Guerin, *A Framework for Policy-based Admission Control*, RFC 2753, January 2000.

[47] D. Durham, Ed., *The COPS (Common Open Policy Service) Protocol*, RFC 2748, January 2000.

13 ABBREVIATIONS AND TERMS

ADSL	Asymmetric Digital Subscriber Lines
AF PHB	Assured Forwarding PHB
API	Application Programming Interface
ARP	Address Resolution Protocol
AS	Autonomous Systems
ATM	Asynchronous Transfer mode
BA	Behaviour Aggregate
BB	Bandwidth Broker
BGP	Border Gateway Protocol
BLOS	Beyond Line-of-Sight
CDN	Content Delivery Network
CL	Connection Less
CNET	Circuit Network
CO	Connection Oriented
COPS	Common Open Policy Service Protocol
COTS	Common Off The Shelf
CU	Currently Unused
DEN	Directory Enable Networking
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DMTF	Distributed Management Task Force
DNS	Domain Name System
DoD	Department of Defence
DSCP	Differentiated Services Code Point
ECN	Explicit Congestion Notification
EF PHB	Expedited Forwarding PHB
E2E	End-to-end
E2N	End to Network
FA	Foreign Agent
FDN	Forsvarets Data Nettverk
FNBDT	Future Narrow Band Digital Terminal
GIG	Global Information Grid
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
HA	Home Agent
HAIPE	NSA High Assurance IP Encryption
HF	High Frequency
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol

INSC	Interoperable Networks for Secure Communications
IntServ	Integrated Services
IOP	InterOperability Point
IP	Internet Protocol
IPR	International Property Rights
IPsec	IP Security
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System to Intermediate System
JTRS	Joint Tactical Radio System
LAN	Local Area Network
LAS	Local Area Systems
LDAP	Lightweight Directory Access Protocol
LOS	Line-of-Sight
LSP	Label Switching Path
LUNAR	Lightweight Underlay Network Ad-Hoc Routing
MAC	Medium Access Control
MBGP	Multi-protocol BGP
MLEF PHB	Multi-Level Expedite Forwarding PHB
MOTS	Military Off The Shelf
MPLS	Multi Protocol Label System
MPLS-TE	MPLS Traffic Engineering
MS	Mobile Systems
MSDP	Multicast Source Discovery Protocol
MSPP	Multi Service Provisioning Platform
NAT	Network Address Translation
NCW	Network Centric Warfare
NE	Network Elements
NEMO	Network Mobility
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PBN	Policy Based Networking
PBQM	Policy Based QoS Network Management
PDH	Plesichronous Digital Hierarchy
PDP	Policy Decision Points
PEP	Policy Enforcement Points
PHB	Per Hop Behaviours
PIM-SM	Protocol Independent Multicast - Sparse Mode
PNET	Packet Network
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAPNET	Radio Access Packet Network
RPF	Reversed Path Forwarding
RSVP	Resource reSerVation Protocol
RTP	Real Time Protocol
SDH	Synchronous Digital Hierarchy
SIP	Session Initiation Protocol
SLA	Service Level Agreements
SSM	Source Specific Multicast

TDM	Time Division Multiplexing
Tetra	Terrestrial Trunked Radio
TITAAN	Theatre-Independent Tactical Army/Air Force Network
TTL	Time To Live
UAV	Unmanned Airborne Vehicles
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over IP
VPN	Virtual Private Network
WAS	Wide Area Systems

APPENDIX

A NAMING AND ADDRESSING

The default naming and addressing structure in the Internet is hierarchal logical names of interfaces and service locations represent the top level. In principle the service maps to a port number and server name, while the logical name maps to an IP address. The IP address has a hierarchal structure determined by the address allocation process. The IP address maps into a flat hardware address space for the interface, the MAC address.

The IP address was originally a stable identifier defining a logical network location. That semantic meaning is being eroded by dynamic address allocation and network address translation towards being part of a flow identifier.

IPv6 addresses have an in-between status. Some proposals suggest using the address as an identifier, while others suggest letting the address contain routing information.

The IP address is used for identification of flow for resource allocation, for classification in per packet scheduling and filtering, and for the forwarding decision. The forwarding decision is not only based on destination address, but also the source address and port numbers. The latter is used in policy-based forwarding and reversed path checking in multicast.

IP multicast addresses are allocated from a selected range in the IP address space (224 and onwards). The multicast addresses do not signal location. Instead, they are used to identify a session or broadcast protocol functions. Multicast addresses need not be unique, since the sessions can be scoped to remain within a boundary. The dynamic allocation of multicast addresses is an operational weakness in multicast. Therefore IETF has an ongoing effort to define address allocation schemes.

A.1 IP address allocated by location

The IP address can be allocated either based on location or identity. The latter will typically be organized according to some organizational scheme. Since organizational units sometimes are along geographically boundaries, the two schemes may look to be identical. However, the scaling implications are different. If addresses in the same location are similar, they can be represented in an aggregated fashion for forwarding and possibly filtering and allocation decisions. However, the dynamic requirement on allocation and authorization imply that these decisions will be made on an individual basis, where aggregation is infeasible. The allocation and authorization process will be of the positive type, i.e. only the ones selected for preferential treatment will be identified. At least on the edges and first tiers of the network, the scaling will not be an issue.

The identity of a terminal, user, or server is represented by a logical name. The name is mapped to an IP address through the naming system. In many networks, the name-address

mapping is part of an overall directory system. When the address is changed due to a change in location, the directory system needs to be updated. However, the naming is based on a substantial use of cashing, so the updating of the mapping can only be done within restrictions on frequency, context, and availability. Specific mobility functions to support changes in location are therefore needed.

In a NCW network, ad hoc networking will be a requirement. In principle, the ad hoc network is a location, and all nodes in the network should have addresses belonging to the ad hoc network. However, this may cause unnecessary strain on the naming resolution and updating. Alternatively, the nodes in the ad hoc network are handled through the mobility scheme. Typically, mobility scheme are based on tunnelling from a home location to the current location. In an ad hoc network, such a solution may imply unnecessary tunnelling of the ad hoc network for internal traffic in the ad hoc network. Location based addressing and ad hoc networks will therefore require more tailor made solutions.

A.2 IP address allocated as an identifier

The IP address can also be used as an equipment identifier. This is similar to the role phone numbers have in cellular systems or to some extents in the fixed phone network (as a consequence of number portability). The forwarding process cannot be based on aggregation of addresses to the same location. In principle, all routers will have to treat the address space as flat. Although, this is not a severe restriction on the backbone routers in a Norwegian NCW network, it has implications on the amount of routing traffic to edge and tier 1 routers. All routers within a domain will have to track all equipment in the domain. The amount of routing traffic will therefore grow exponentially with the number of equipment. The routing tables at the edges where the number of alternatives are restricted can still be organized fairly compactly. Furthermore it implies that all end systems must contain its own routing process, since a subnetwork address is meaningless when addresses are just identifiers. For filtering and allocation, the IP address is used as an identifier, and there should be no consequences.

At least initially, the mobility will be moderate. If the allocation of identifiers follows organizational boundaries, there can be substantial degree of aggregated route representation and default routing. In an ad hoc network setting, the routing is based on a flat address space, and IP addresses allocated as identifiers represent no additional problem. Similarly, the mapping of logical name to address is limited to support for users changing their terminal. In all other cases, the mapping is constant.

The disadvantage of using IP addresses as identifiers is the scaling issues associated with forwarding. It is also contrary to the Internet philosophy, and there might be a mismatch between the actual usage of the various protocols and their intended usage. The routing process will handle all mobility issues, since the granularity of the routing process is the individual address.

A.3 Alternative IP address allocation schemes

The two schemes can be combined, with IP address based on location for mostly fixed equipment, while IP address based on identifier for equipment used mostly in ad hoc networks. However, this implies that all routing, naming and mobility methods must be geared for handling both types. This will tend to result in processes that are more complex since two different sets of disadvantages must be countered.

A.4 IP address allocation and international cooperation

In multinational operations, Norwegian NCW network elements will be integrated with other national networks. When the interfacing is along administrative network boundaries, the IP allocation scheme will be a network internal procedure. The interface to other networks will be over a well-defined interdomain interface. The allocation scheme is then of no particular interest, since it is not visible across the interface. However, if Norwegian NCW equipment is integrated into a multinational network, the administrator of the multinational network will determine the IP address allocation.

A.5 Conclusion for IP address allocation

Since IP addresses will be allocated within the same administrative domain, it is doable to change allocation scheme. Initially, the usage of mobility and ad hoc networking will be limited. The COTS or MOTS routers will be designed for aggregated IP addresses. The prudent scheme is therefore to use IP address allocation based on location. Later on, when the usage of mobility and ad hoc networking is more substantial, the decision can be revised, since it is fairly simple to change allocation based on location to allocation based on identifiers; the old location can simply be used as the allocation key in the identifier based scheme.